MG-SOFT Corporation

Net Inspector
Performance Manager 2015

USER MANUAL

(Document Version: 10.6)

Document published on October 16, 2015

Copyright © 1995-2015 MG-SOFT Corporation

In order to improve the design or performance characteristics, MG-SOFT reserves the right to make changes in this document or in the software without notice.

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of MG-SOFT Corporation. Permission to print one copy is hereby granted if your only means of access is electronic.

Depending on your license, certain functions described in this document may not be available in the version of the software that you are currently using.

Screenshots used in this document may slightly differ from those on your display.

MG-SOFT may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. The furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Copyright © 1995-2015 MG-SOFT Corporation. All rights reserved.

TABLE OF CONTENTS

1 Introduction 6

2 Viewing Performance Manager Website 7

2.1 Opening Performance Manager Home Page 7

2.2 About Performance Manager Website 8

3 Network Monitoring 10

3.1 Viewing Alarms 10

3.2 Monitoring Device Status 11

3.3 Viewing Device Performance Data 12

System Information and Responsiveness 16

Memory and Processor Usage Statistics 18

Storage Usage Statistics 18

Services Statistics 18

Processes Statistics 19

Network Interfaces Statistics 20

IP SLA Statistics 20

Device-Related Alarms 22

Custom Statistics 22

3.3.1 Editing Device Performance Page Layout 23

To Edit the Device Performance Page Layout: 23

To Revert the Device Performance Page Layout to Default Settings: 25

3.3.2 Configuring Device Monitoring Options (Interfaces, Storage Units, Processes, Services) 26

3.4 NetFlow / sFlow Monitoring 30

3.4.1 NetFlow Home Page 30

About NetFlow Data Aggregation 33

3.4.2 Router Details Page 33

3.4.3 Interface Details Page 35

3.4.4 Conversation Details Page 35

3.4.5 Endpoint Details Page 38

3.4.6 Protocol Details Page 39

3.4.7 Country Details Page 40

3.4.8 Application Details Page 42

3.4.9 NetFlow Configuration Page 43

3.5 Monitoring Network Services 44

3.6 IP SLA Monitoring 46

4 Viewing and Creating Reports 48

4.1 Viewing Predefined Reports 48

4.2 Creating Custom Reports 50

4.2.1 Creating Custom Report Pages 51

4.3 Editing Custom Report Pages 54

To Add New Object (Table or Graph) to Page 55

To Add New Line to Graph 56

4.3.1 Creating Map Report Page 58

4.3.2 Monitoring Devices on Map 61

4.4 Creating PDF Reports 62

5 Viewing Number of Monitored Objects 64

TABLE OF FIGURES

Figure 1: Accessing Performance Manager website in Net Inspector Client 7
Figure 2: Net Inspector Performance Manager – displaying user's home page (default) 8
Figure 3: Viewing alarms 10
Figure 4: Monitoring devices 12
Figure 5: Opening Performance Statistics window for the selected device 13
Figure 6: An example of device performance page, upper part (single column page layout) 14
Figure 7: An example of device performance page, lower part (single column page layout) 17
Figure 8: Services frame in the device performance page 18
Figure 9: Example of a web page with process statistics 19
Figure 10: Example of a web page with network interface statistics 20
Figure 11: VoIP frame in the device performance page 21
Figure 12: Example of a web page displaying the IP SLA VoIP quality statistics 21
Figure 13: Alarms frame in the device performance page 22
Figure 14: Selecting the Edit page layout link in the device performance page 23
Figure 15: Opened Edit page layout drop-down frame in the device performance page 23
Figure 16: Repositioning a frame using the drag&drop technique 24
Figure 17: Applying the new page layout to the selected device 25
Figure 18: Closing the Edit page layout drop-down frame 25
Figure 19: Restoring the page layout to default settings 25
Figure 20: Choosing the Configure button in the device performance page 26
Figure 21: Edit Device Monitoring Options page - Interfaces tab 27
Figure 22: Edit Device Monitoring Options page - Storage tab 27
Figure 23: Edit Device Monitoring Options page - Processes tab 28
Figure 24: Edit Device Monitoring Options page - Services tab 29
Figure 25: Click the "NF" toolbar button in Net Inspector Client to open the NetFlow home page 30
Figure 26: NetFlow home page displays consolidated NetFlow reports 32
Figure 27: Detailed NetFlow Information 33
Figure 28: Router Details page 34
Figure 29: Interface Details page 35
Figure 30: Conversation Details page 36
Figure 31: Zooming in the conversation details graph 37
Figure 32: Zoomed in conversation details graph (note the 5 min aggregation level of data) 38
Figure 33: Endpoint Details page 39
Figure 34: Protocol Details page 40
Figure 35: Country Details page 41
Figure 36: Application Details page 42
Figure 37: NetFlow Configuration Page 43
Figure 38: Services page 44
Figure 39: Viewing the availability history of a www service 45
Figure 40: Viewing the latency history of a www service (HTTP Get request-response RTT) 45
Figure 41: IP SLA page 46
Figure 42: Example of a web page displaying the IP SLA VoIP quality statistics (MOS) 47
Figure 43: Selecting a predefined time report from the Reports page 49

Figure 44: Viewing a predefined time report (Device Availability) 50
Figure 45: Reports page 51
Figure 46: Setting the number of columns for a custom report page 51
Figure 47: Example of setting a Top5 report properties in the custom page configurator 52
Figure 48: Viewing custom report page containing one object (table) 53
Figure 49: Reports page with one custom report page 54
Figure 50: Opening a custom report page 54
Figure 51: Viewing a custom report page in page configurator 55
Figure 52: Configuring a second object in the custom report page 55
Figure 53: Custom report page with two objects (tables) in a row 56
Figure 54: Clicking the Add Variable button in an existing graph 57
Figure 55: Adding a new variable to the existing graph 57
Figure 56: Viewing a graph chart containing two variables 58
Figure 57: The Reports home page 58
Figure 58: Device map report configurator 59
Figure 59: Device map report configurator (second page) 60
Figure 60: Viewing a device map report page. 61
Figure 61: Generating a PDF report 62
Figure 62: Viewing Custom report page in PDF format 63
Figure 63: A PDF report in the Reports page 63

1 INTRODUCTION

This guide contains instructions for completing basic operations in MG-SOFT Net Inspector Performance Manager application, which makes an integral part of the MG-SOFT Net Inspector Fault and Performance Manager package (it is integrated in Net Inspector WorkGroup, Enterprise and Carrier Edition software packages).

Majority of instructions are provided on a step-by-step basis, which should help the reader start using the software effectively.

It is presumed that you are familiar with using a graphical computer environment, especially using a web browser application. MG-SOFT Net Inspector Performance Manager has a web-based graphical front-end.

All program commands in this manual are written in bold and italic letters. Individual commands in combinations of commands are separated by the "/" character.

All hyperlinks in text are marked with blue colored letters, e.g., Creating Reports. Clicking a hyperlink opens the page which the hyperlink points to.

The content of this guide is listed in the Table of Contents.

2 VIEWING PERFORMANCE MANAGER WEBSITE

MG-SOFT Net Inspector Performance Manager module has a web-based graphical front-end, which lets you monitor the status and performance of your network. The Web pages generated by a Performance Manager module are accessed from the Net Inspector Client application, as follows:

First, launch the Net Inspector Client application and log on to Net Inspector Server as described in the "**Net Inspector Getting Started Guide**" document in the following sections:

- Starting Net Inspector Client
- Connecting Net Inspector Client to Server

2.1 Opening Performance Manager Home Page

To open the Performance Manager Home Page, from where you can access all other Web pages generated by the specific instance of Net Inspector Performance Manager, proceed as follows:

1. In Net Inspector Client, select the ***Tools / Show Performance Manager*** command from the main menu or click the ***Show Performance Manager*** toolbar button (Figure 1).

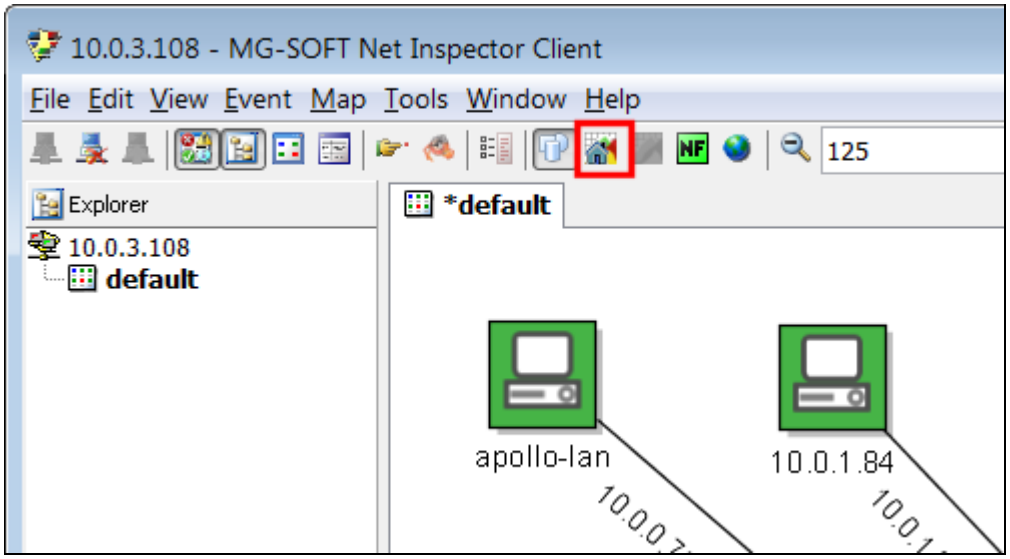


Figure 1: Accessing Performance Manager website in Net Inspector Client

2. The MG-SOFT Net Inspector Performance Manager website, user home page is displayed in the Java-based Web browser window within the Net Inspector application (Figure 2).

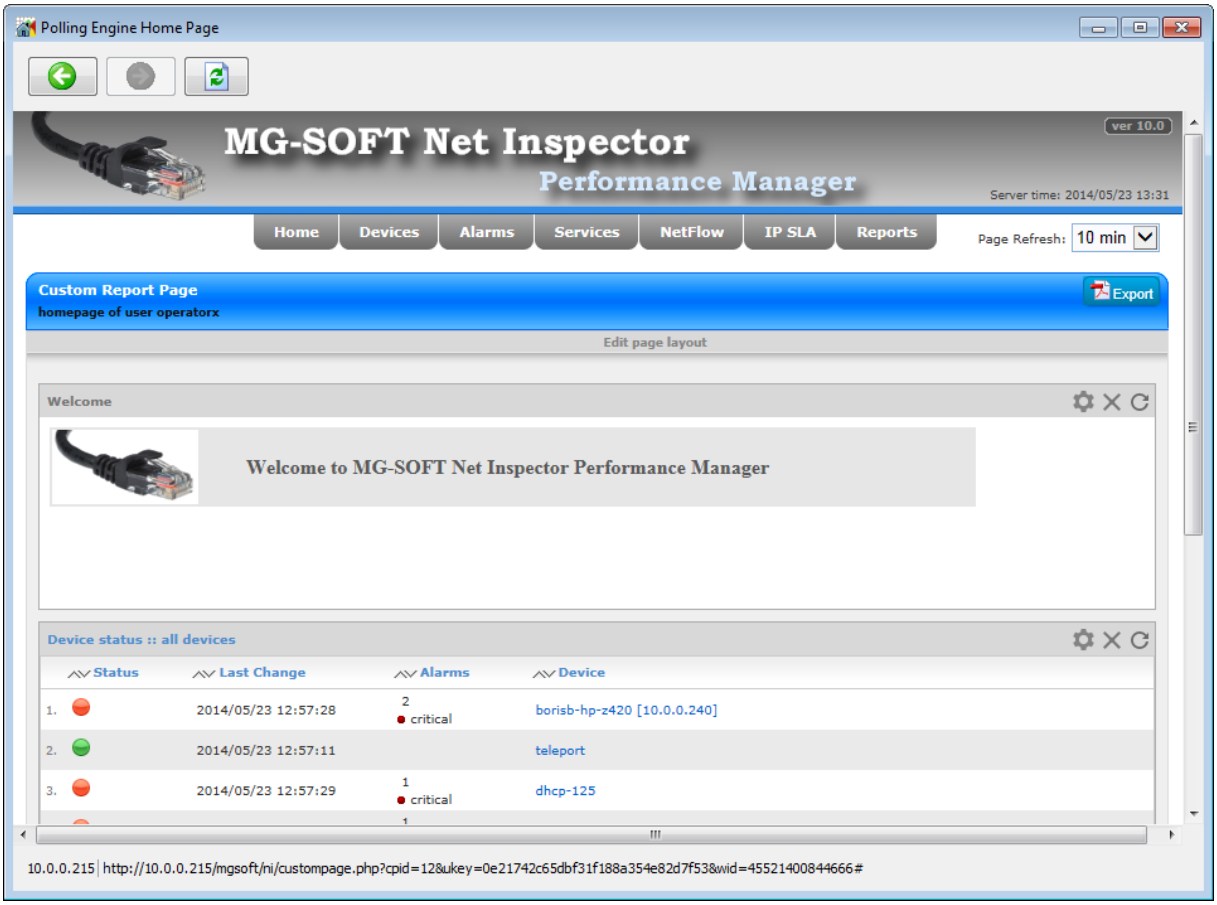


Figure 2: Net Inspector Performance Manager – displaying user's home page (default)

By default, user home page contains the Welcome frame and the Device status frame displaying a list of all devices in the active user view and their current status. You can customize your home page, for example, to include different or additional information.

To start customizing the home page, click the ***Edit page layout*** link below the title bar of the user home page frame. Follow the guidelines in the Editing Custom Report Pages section of this manual.

2.2 About Performance Manager Website

MG-SOFT Performance Manager website contains several sections. You can switch between them by clicking the following **tabs** displayed in the top section of each Web page (Figure 2):

Home
When you click this tab, your home page is displayed (Figure 2). Every Net Inspector user has its own home page, which is displayed automatically when the user opens the Net Inspector Performance Manager website. Home pages can be customized to contain one or more custom reports (graphs, tables), external web pages (included as HTTP frames), and/or a map on which the user can drag-and-drop icons of devices and monitor their status. User home pages fall into category of custom report pages and are configured in the same manner.

Devices
When you click this tab, the Performance Manager Devices page is displayed, where you can view all monitored devices included in the currently active Net Inspector user view, the current status of devices, assigned polling engine, and the basic device alarm information (the number of alarms and severity of the most critical alarm associated with the device).

Alarms
When you click this tab, the Performance Manager Alarms page is displayed. The Alarms page displays all active (open) alarms associated with the devices. New alarms will be automatically added to the Alarms list as they occur (after web page refresh), and the existing alarms will disappear from the list (after web page refresh) when they are cleared.

Services
When you click this tab, the Performance Manager Services page is displayed. The Services page displays a list all monitored services on devices by service category (DNS, HTTP, IMAP, SSH,…) and a list of services with status “Critical”. By clicking a service on the list, more detailed statistics for the selected service is displayed (service availability and round trip time (RTT)).

NetFlow
When you click this tab, the Performance Manager NetFlow page is displayed. The NetFlow page displays the list of all configured NetFlow and sFlow source devices (if any) and the TopN NetFlow traffic reports for all NetFlow sources. By expanding and clicking the individual subentries in the Top N reports, more detailed statistics for the selected item (e.g., device, interface, conversation, application, etc.) is shown.

IP SLA
When you click this tab, the Performance Manager IP SLA page is displayed. The IP SLA page displays the lists of the IP SLA operations monitored on your (Cisco) devices and related statistics (e.g., round trip times, jitter, packet loss, etc.).

Reports
When you click this tab, the Performance Manager Reports page is displayed. The Reports page contains a series of predefined fault and performance management reports (e.g., device availability, number of alarms per severity, network interface utilization,…). In addition, the Report page lets you configure also custom reports, containing graphs or tables displaying metrics monitored on one or more devices. Examples of such custom reports are Top10 reports, reports of monitored objects with problems, etc..

3 NETWORK MONITORING

3.1 Viewing Alarms

Click the ***Alarms*** tab to display the Alarms page (Figure 3).

MG-SOFT Net Inspector
Performance Manager
ver 8.0
Server time: 2011/05/31 01:24
System summary
Home
Devices
Alarms
NetFlow
IPSLA
Reports
Page Refresh: 10 min
Alarms
Time
Description
Severity
Device
Source Info
Value
2011/05/30 22:35:08 [10002] SNMP agent not responding major teleport
2011/05/30 22:35:08 [10002] SNMP agent not responding major kasiopea
2011/05/30 22:35:08 [10002] SNMP agent not responding major galileo
2011/05/30 22:35:08 [10002] SNMP agent not responding major hercules
2011/05/30 22:35:08 [10002] SNMP agent not responding major turtle
2011/05/30 22:35:09 [10002] SNMP agent not responding major camserver
2011/05/30 22:35:09 [10002] SNMP agent not responding major ciscoSwitch2
2011/05/30 22:35:13 [10002] SNMP agent not responding major tadejm-hp
First Prev 1 Next Last
Copyright (C) 2011 MG-SOFT. All rights reserved.

Figure 3: Viewing alarms

The Alarms page displays all active (open) alarms. New alarms will be automatically added to the Alarms list as they occur (after web page refresh), and the existing alarms will disappear from the list (after web page refresh) when they get cleared.

Note 1: **Alarms** are messages that indicate faults or conditions that could lead to faults on managed devices. An alarm can be **active** or **cleared**. An alarm is active as long as the condition that triggered it is present (e.g., when a managed device does not respond to queries, the "Device is down" alarm is raised and becomes active; when the device starts responding again, the "Device is down" alarm is cleared).

Note 2: **Only active alarms are displayed in the Alarms page.**

Every line in the Alarms list represents one alarm. Alarms provide the following information:

`Time`	Date and time when the alarm occurred
`Description`	Short description of the alarm
`Severity`	Severity of the alarm

`Device`	Name of the device associated with alarm
`Source Info`	Additional information about the source of alarm
`Value`	Value of the threshold variable (for threshold alarms only)

Alarms are colored according to their severity levels:

The alarm severity levels, their symbols and colors (listed from least to most severe)

While the severity level assigned to pre-defined alarms cannot be changed, you can assign any severity level to user-defined alarms.

- Click the **sort** toggle symbol ( ) in the column header (`Time`, `Description`, `Severity`) to sort alarms by that column in ascending or descending order.
- Set the global page refresh interval to the desired value (e.g., `1 min`, `3 min`, `5 min`, `10 min`, ...) by selecting it from the ***Page Refresh*** drop-down list next to the **Settings** tab in the upper-right section of the page.
- To manually refresh the alarms list, use the web browser's ***Refresh*** (typically ***CTRL+R***) command.
- To view the web page dedicated to device, which the alarm is related to, click the device name hyperlink in the ***Device*** column of the **Alarms** page.

3.2 Monitoring Device Status

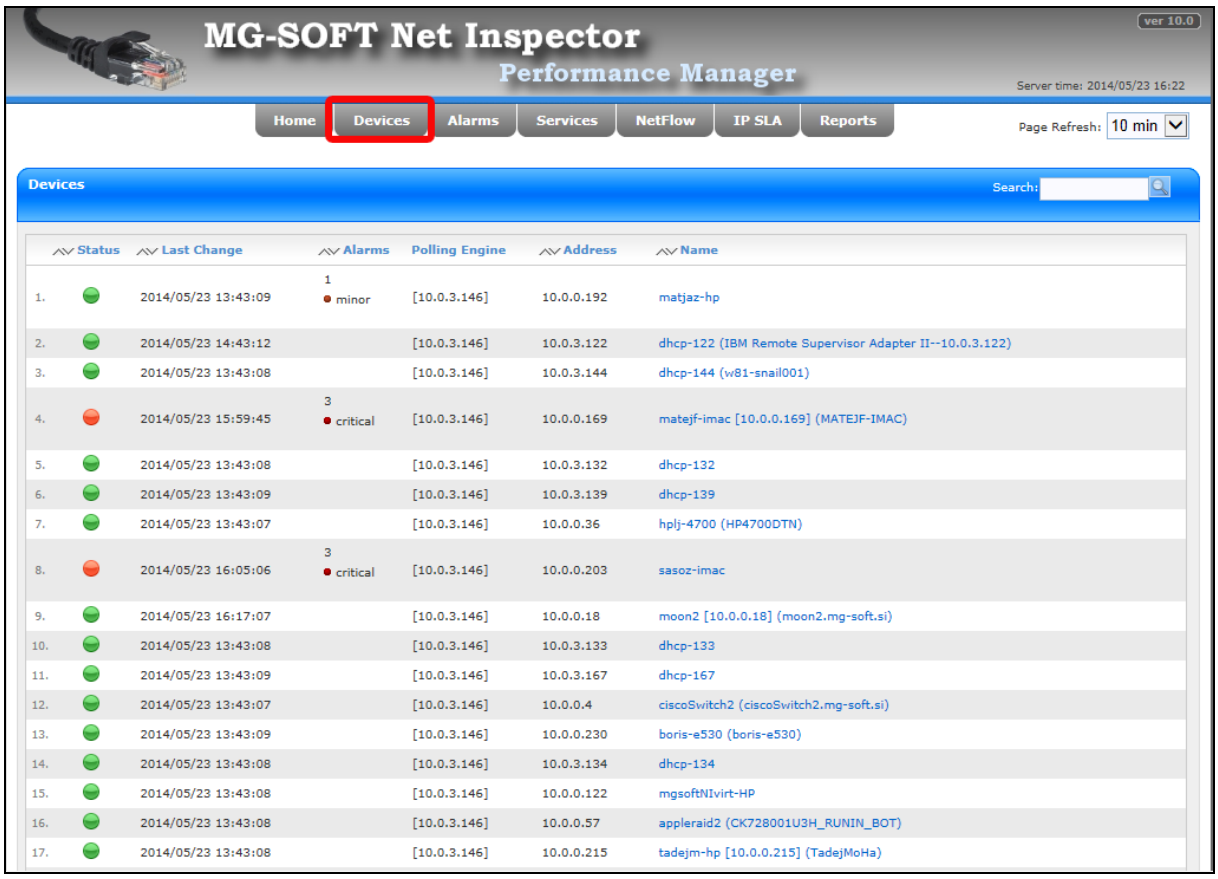
Click the ***Devices*** tab in the main window to display the Devices page (Figure 4).

The Devices page displays a list of all devices in the currently active user view. The ***Name*** column displays the hostname (if available) of each device and the value of its sysName.0 object instance (if available) in round brackets. If a device has more than one IP address assigned, the IP address used for monitoring the given device is displayed in square brackets next to the hostname.

The Devices page provides information about the current status of each device (***Status*** column), the alarms associated with each device (***Alarms*** column), the name and address of each device, as well as the address of the polling engine used for poling each device.

The following symbols are used to indicate the **status** of devices (***Status*** column):

- - device is up (responding)
- - device is down (not responding)
- - device monitoring is disabled



	Status	Last Change	Alarms	Polling Engine	Address	Name
1.		2014/05/23 13:43:09	1 minor	[10.0.3.146]	10.0.0.192	matjaz-hp
2.		2014/05/23 14:43:12		[10.0.3.146]	10.0.3.122	dhcp-122 (IBM Remote Supervisor Adapter II--10.0.3.122)
3.		2014/05/23 13:43:08		[10.0.3.146]	10.0.3.144	dhcp-144 (w81-snail001)
4.		2014/05/23 15:59:45	3 critical	[10.0.3.146]	10.0.0.169	matejf-imac [10.0.0.169] (MATEJF-IMAC)
5.		2014/05/23 13:43:08		[10.0.3.146]	10.0.3.132	dhcp-132
6.		2014/05/23 13:43:09		[10.0.3.146]	10.0.3.139	dhcp-139
7.		2014/05/23 13:43:07		[10.0.3.146]	10.0.0.36	hplj-4700 (HP4700DTN)
8.		2014/05/23 16:05:06	3 critical	[10.0.3.146]	10.0.0.203	sasoz-imac
9.		2014/05/23 16:17:07		[10.0.3.146]	10.0.0.18	moon2 [10.0.0.18] (moon2.mg-soft.si)
10.		2014/05/23 13:43:08		[10.0.3.146]	10.0.3.133	dhcp-133
11.		2014/05/23 13:43:09		[10.0.3.146]	10.0.3.167	dhcp-167
12.		2014/05/23 13:43:07		[10.0.3.146]	10.0.0.4	ciscoSwitch2 (ciscoSwitch2.mg-soft.si)
13.		2014/05/23 13:43:09		[10.0.3.146]	10.0.0.230	boris-e530 (boris-e530)
14.		2014/05/23 13:43:08		[10.0.3.146]	10.0.3.134	dhcp-134
15.		2014/05/23 13:43:08		[10.0.3.146]	10.0.0.122	mgsoftNIvirt-HP
16.		2014/05/23 13:43:08		[10.0.3.146]	10.0.0.57	appleraid2 (CK728001U3H_RUNIN_BOT)
17.		2014/05/23 13:43:08		[10.0.3.146]	10.0.0.215	tadejm-hp [10.0.0.215] (TadejMoHa)

Figure 4: Monitoring devices

The ***Alarms*** column displays the number of active alarms associated with the device and severity level of the most severe alarm.

- To sort devices by a column in ascending/descending order, click the **sort** toggle symbol ( ) in the corresponding column header. For example, to quickly view all devices with the status of critical, sort devices by status by clicking the **sort** toggle symbol ( ) in the ***Status*** column header.
- To find a particular device by its name or to filter devices by the name based on the string the name contains, enter the string (e.g., device name or part of it) into the ***Search*** input line in the titlebar of the Devices page.
- To view a device-related web page and the data collected from a device through polling, click on a device name hyperlink in the ***Name*** column.

3.3 Viewing Device Performance Data

In Net Inspector WorkGroup Edition and better (which integrate the Performance Manager functionality) managed objects are polled by Performance Manager polling engine by default (as opposed to the Net Inspector LITE Edition, where polling is performed by the Net Inspector Server itself). In such configuration, detailed device performance statistics with history can be viewed in the Performance Statistics window, as described in this section.

1. In the Net Inspector Client application, open the map that contains the managed object(s) you want to view the properties of by expanding the hierarchical map tree in the Explorer window (***View / Explorer***), selecting the relevant map and choosing the ***Open*** pop-up command.
2. A new tab opens in the Maps window, displaying the managed objects (and submaps if any) contained in the selected map.
3. To open the Performance Statistics window and view the performance data of the selected managed object, select a managed object and choose the ***Show Performance Statistics*** pop-up command (Figure 5).

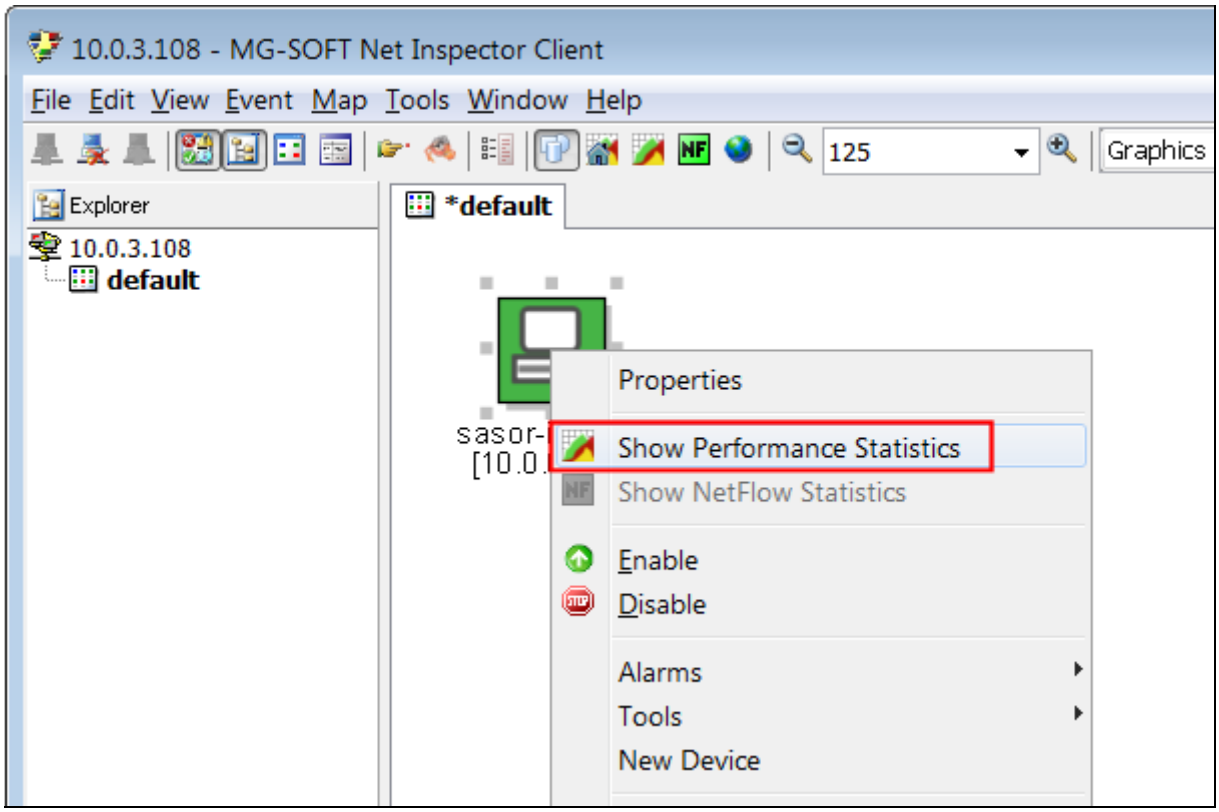


Figure 5: Opening Performance Statistics window for the selected device

4. The device performance web page for the selected device is displayed (Figure 6).

Alternatively, device performance statistics can be viewed by clicking a device name hyperlink on the Devices page.

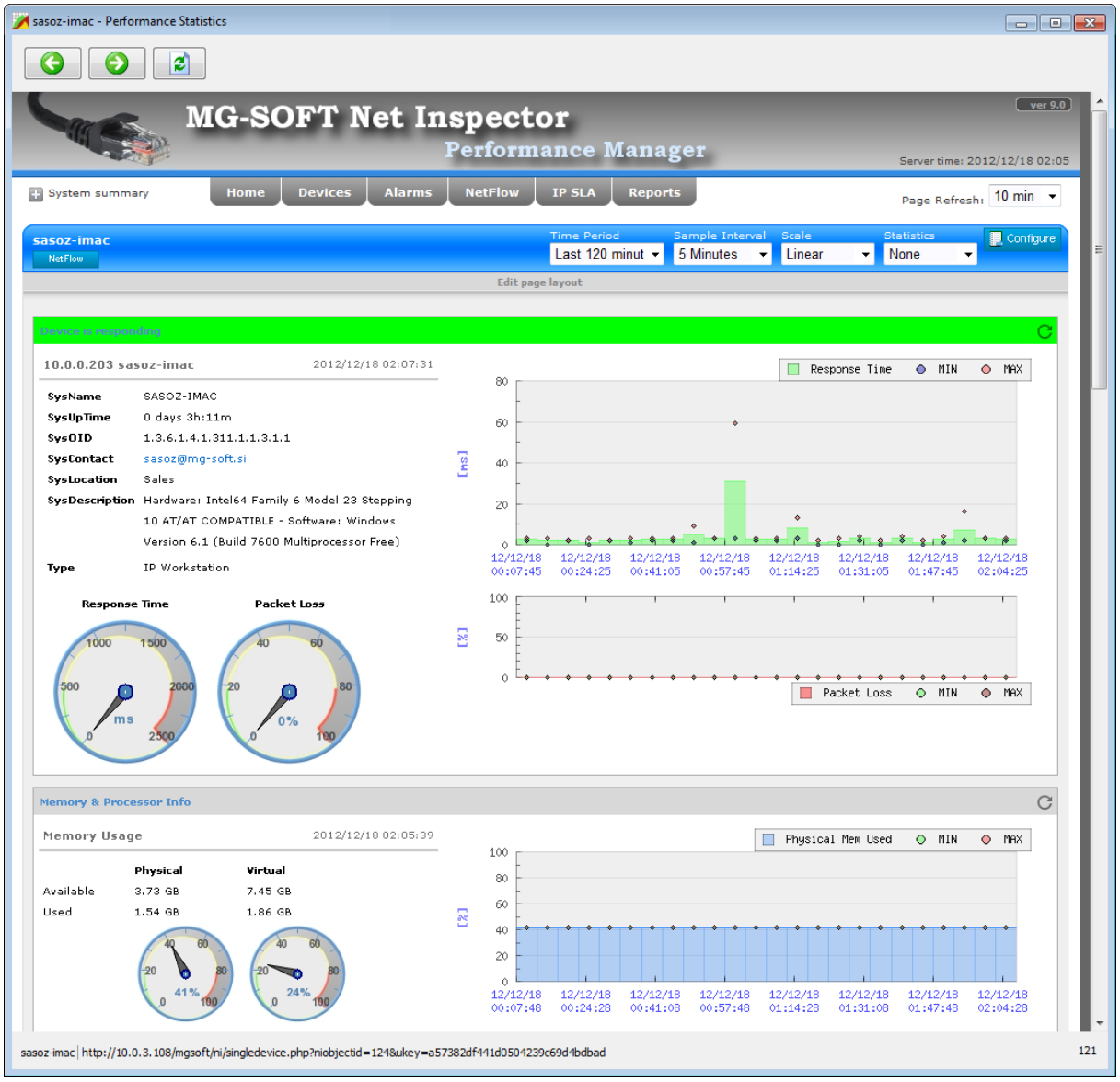


Figure 6: An example of device performance page, upper part (single column page layout)

The contents (displayed categories) and the layout (order of categories, number of columns) of the device performance page can be customized to meet your preferences, as described in the Editing the Device Performance Page Layout section.

By default, the device performance page displays the system information, response times (average, min., max.) and packet loss rate for the selected device, as well as the status of monitored network services and utilization rates of network interfaces on that device. For devices implementing the HOST-RESOURCES-MIB module and for Cisco devices, this page displays also Memory & Processor Info (memory usage, CPU load), Storage Info and Process information (process name, path, PID, CPU and memory consumption) provided that monitoring of all these metrics is enabled in the polling profile that is assigned to the given device.

By default, the device performance page displays all device-related alarms (Figure 13).

In addition to displaying the last retrieved device performance values, this report page shows also history graphs for the **response time**, **packet loss**, **memory usage**, and **CPU load** variables (where applicable).

By default, graphs display monitored variables for the last 120 minutes. To use a different time frame, select the corresponding entry from the ***Time period*** drop-down list in the device performance toolbar (e.g., last 60 minutes, yesterday, last 7 days, last 30 days, etc.). All graphs in the device performance page will be updated to show variables for the selected time frame. The following entries can be selected from the ***Time period*** drop-down list:

Example: Current Date/Time: Tue, 2010/10/05 14:45:00

Time Period	Example Start Date/Time	Example End Date/Time
This hour	2010/10/05 14:00:00	2010/10/05 15:00:00
Last 60 minutes	2010/10/05 13:45:00	2010/10/05 14:45:00
Last hour	2010/10/05 13:00:00	2010/10/05 14:00:00
***Last 120 minutes**	2010/10/05 12:45:00	2010/10/05 14:45:00
Today	2010/10/05 00:00:00	2010/10/06 00:00:00
Yesterday	2010/10/04 00:00:00	2010/10/05 00:00:00
This week	Mon, 2010/10/04 00:00:00	Mon, 2010/10/11 00:00:00
Last 7 days	2010/09/29 00:00:00	2010/10/06 00:00:00
Last week	Mon, 2010/09/27 00:00:00	Mon, 2010/10/04 00:00:00
Last business week	Mon, 2010/09/27 00:00:00	Sat, 2010/10/02 00:00:00
Last 14 days	2010/09/22 00:00:00	2010/10/06 00:00:00
This month	2010/10/01 00:00:00	2010/11/01 00:00:00
Last 30 days	2010/09/06 00:00:00	2010/10/06 00:00:00
Last month	2010/09/01 00:00:00	2010/10/01 00:00:00

The Date/Time format is: YYYY/MM/DD HH:mm:ss

***** Default time period

By default the graphs sampling interval is set to 5 minutes. To use a different sampling interval, select a corresponding entry from the ***Sample Interval*** drop-down list in the device performance toolbar (e.g., 1 minute, 5 minutes, 30 minutes, 1 hour, 6 hours, 12 hours, 1 day). All graphs in the device performance page will be updated to show data in the selected sampling interval.

The sampling interval determines the granularity of the data shown, i.e., how many bars in graphs or lines in tables are shown per given time period. For example, if the time period is set to *Last 60 minutes*, and the sample interval is set to *5 minutes*, the graphs will display 12 bars within one hour interval (60/5=12). The graph bars and values in tables display the **average values** within the sampling intervals.

Note: About data aggregation and values displayed

For all metrics shown in device performance web pages (e.g., response time, CPU load, interface utilization, MOS, etc.) the collected values are being gradually aggregated, meaning that from individual readings, average values are being calculated and displayed in graphs and tables, depending on the time period and the sampling interval set.

Note: About data aggregation and values displayed - *continued*

By default, the following aggregation model is used for performance data (a different model is used for NetFlow data):

* The values for the last 7 days are kept unmodified in the database (**raw data** without aggregation).
* For the period between the last 32 days and last 7 days, only the **hourly averages** are kept in the database.
* For the period between the last 366 days and last 32 days, only the **daily averages** are kept in the database.

The graph bars and table values in device performance web pages always display the **average values** of readings within sample intervals, for example, if the polling interval is 1 minute and the sampling interval is 5 minutes, then each graph bar and table value will show the average value of 5 readings (approximately). By setting the sampling interval to equal to or less than polling interval (for any period within the last 7 days for which the raw data is kept by default), one can view the actual raw data (individual readings collected from devices).

In addition to average values, the absolute maximum (**MAX**) and minimum (**MIN**) values are shown in graphs and tables for each sampling interval.

You can also set the linear or logarithmic scale for graphs by selecting the respective entry from the ***Scale*** drop-down list in the device performance toolbar.

Furthermore, you can add a 95-percentile line, a trend line or both to the graph by selecting the respective entry from the **Statistics** drop-down list in the device performance toolbar.

Note: 95-percentile and trend lines

A percentile is the value of a variable below which a certain percent of observations fall. Therefore, the 95-percentile line is a line under which you will find 95% of observations.

Trend line is a straight line connecting multiple points on a chart. A trend line is used in technical analysis to determine the direction and strength of a trend. An up trend line has a positive slope and connects at least two low points on a chart. A down trend line has a negative slope and connects at least two high points on a chart. The steepness of the slope of a trend line indicates the strength of the trend.

To view more detailed graphs and tables for any metric, click on its graph/chart in the device performance page. After clicking on a graph to display it in detailed page, you can zoom into a specific time interval by selecting a specific time period in a graph with your mouse.

System Information and Responsiveness

The **Response Time** frame (Figure 6) in the Performance Statistics window provides the basic information about the given device, its status (titlebar color and text) and ping statistics. This frame provides the general information about the device, like its IP address/hostname, SysName, SysLocation, SysContact, SysDescription, etc. The Sys* data is obtained by querying the standard MIB-II system group of objects via SNMP. The information displayed will depend upon what information is available for

that device in its MIB. The section on the right displays the ping statistics history graphs, i.e. device response times (in milliseconds), and the packet loss rate (in %). The current response time and packet loss rate are presented also in gauge charts.

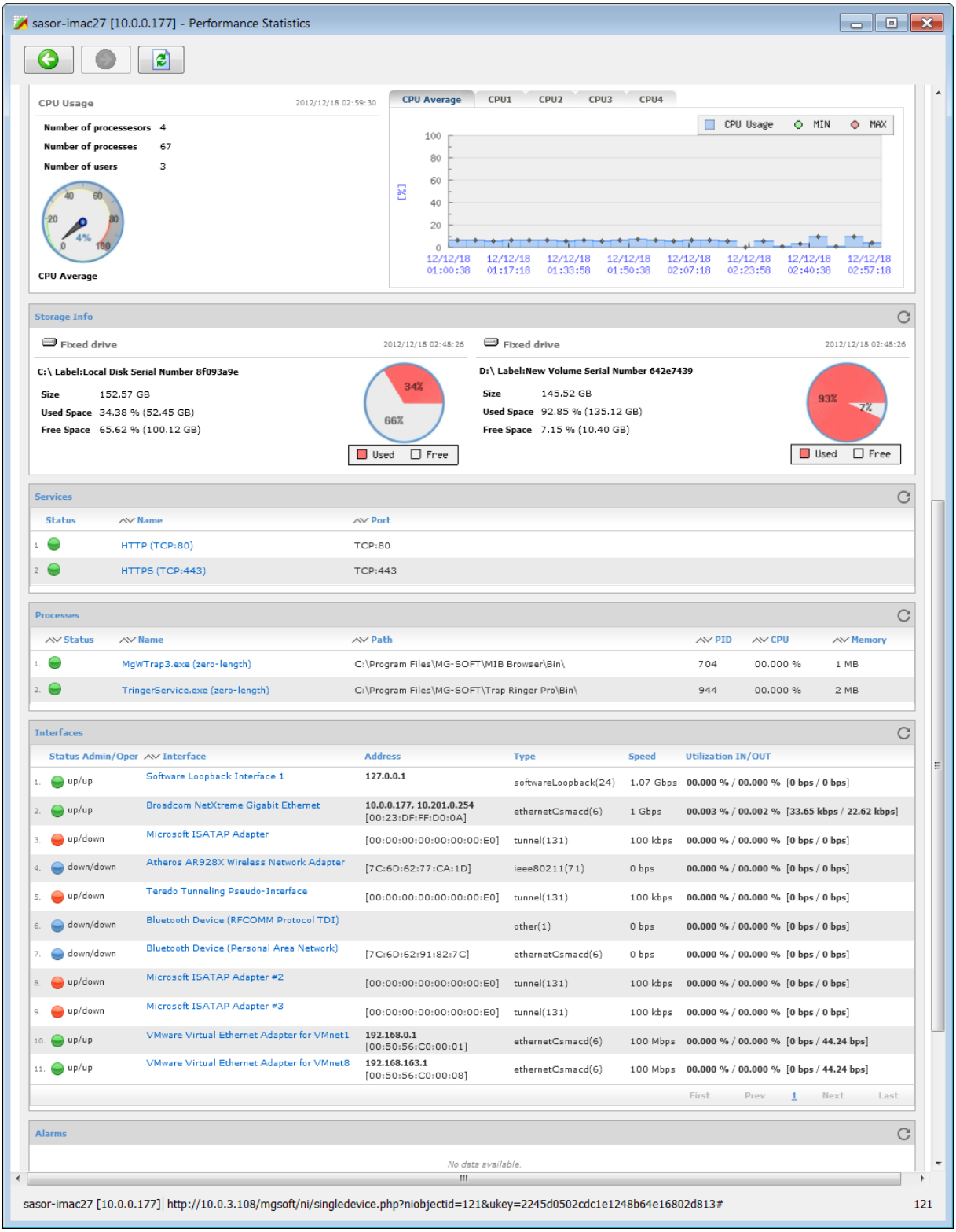

sasor-imac27 [10.0.0.177] - Performance Statistics
CPU Usage
2012/12/18 02:59:30
Number of processesors 4
Number of processes 67
Number of users 3
CPU Average
CPU1
CPU2
CPU3
CPU4
CPU Usage
MIN
MAX
[%]
Storage Info
Fixed drive
2012/12/18 02:48:26
C:\ Label:Local Disk Serial Number 8f093a9e
Size 152.57 GB
Used Space 34.38 % (52.45 GB)
Free Space 65.62 % (100.12 GB)
34%
66%
Used
Free
Fixed drive
2012/12/18 02:48:26
D:\ Label:New Volume Serial Number 642e7439
Size 145.52 GB
Used Space 92.85 % (135.12 GB)
Free Space 7.15 % (10.40 GB)
93%
7%
Used
Free
Services
Status
Name
Port
1 HTTP (TCP:80) TCP:80
2 HTTPS (TCP:443) TCP:443
Processes
Status
Name
Path
PID
CPU
Memory
1. MgWTrap3.exe (zero-length) C:\Program Files\MG-SOFT\MIB Browser\Bin\ 704 00.000 % 1 MB
2. TringerService.exe (zero-length) C:\Program Files\MG-SOFT\Trap Ringer Pro\Bin\ 944 00.000 % 2 MB
Interfaces
Status Admin/Oper
Interface
Address
Type
Speed
Utilization IN/OUT
1. up/up Software Loopback Interface 1 127.0.0.1 softwareLoopback(24) 1.07 Gbps 00.000 % / 00.000 % [0 bps / 0 bps]
2. up/up Broadcom NetXtreme Gigabit Ethernet 10.0.0.177, 10.201.0.254 [00:23:DF:FF:D0:0A] ethernetCsmacd(6) 1 Gbps 00.003 % / 00.002 % [33.65 kbps / 22.62 kbps]
3. up/down Microsoft ISATAP Adapter [00:00:00:00:00:00:00:E0] tunnel(131) 100 kbps 00.000 % / 00.000 % [0 bps / 0 bps]
4. down/down Atheros AR928X Wireless Network Adapter [7C:6D:62:77:CA:1D] ieee80211(71) 0 bps 00.000 % / 00.000 % [0 bps / 0 bps]
5. up/down Teredo Tunneling Pseudo-Interface [00:00:00:00:00:00:00:E0] tunnel(131) 100 kbps 00.000 % / 00.000 % [0 bps / 0 bps]
6. down/down Bluetooth Device (RFCOMM Protocol TDI) other(1) 0 bps 00.000 % / 00.000 % [0 bps / 0 bps]
7. down/down Bluetooth Device (Personal Area Network) [7C:6D:62:91:82:7C] ethernetCsmacd(6) 0 bps 00.000 % / 00.000 % [0 bps / 0 bps]
8. up/down Microsoft ISATAP Adapter #2 [00:00:00:00:00:00:00:E0] tunnel(131) 100 kbps 00.000 % / 00.000 % [0 bps / 0 bps]
9. up/down Microsoft ISATAP Adapter #3 [00:00:00:00:00:00:00:E0] tunnel(131) 100 kbps 00.000 % / 00.000 % [0 bps / 0 bps]
10. up/up VMware Virtual Ethernet Adapter for VMnet1 192.168.0.1 [00:50:56:C0:00:01] ethernetCsmacd(6) 100 Mbps 00.000 % / 00.000 % [0 bps / 44.24 bps]
11. up/up VMware Virtual Ethernet Adapter for VMnet8 192.168.163.1 [00:50:56:C0:00:08] ethernetCsmacd(6) 100 Mbps 00.000 % / 00.000 % [0 bps / 44.24 bps]
First Prev 1 Next Last
Alarms
No data available.
sasor-imac27 [10.0.0.177] http://10.0.3.108/mgsoft/ni/singledevice.php?niobjectid=121&ukey=2245d0502cdc1e1248b64e16802d813# 121

Figure 7: An example of device performance page, lower part (single column page layout)

Memory and Processor Usage Statistics

The **Memory and Processor Info** frame in the device performance web page (Figure 6, Figure 7) displays information only for Cisco devices and devices supporting the standard HOST-RESOURCES-MIB module (like servers, workstations, etc.), provided that the host resources monitoring is enabled in the polling profile assigned to those devices.

This frame displays information about device resources and their utilization rates, i.e., physical memory size and consumption, the number of CPUs, processes and users and the CPU usage. The last-retrieved values are presented in gauge charts, while the history graphs are shown in the right section of the page. Click on a graph to view a web page with history data (in form of a graph and table) for the corresponding metric.

Storage Usage Statistics

The **Storage Info** frame in the device performance web page (Figure 7) displays the monitored storage volumes (logical disks), their names, sizes and current usage (used and free space).

The last-retrieved values are presented in gauge charts. Click a gauge chart to view a web page displaying the storage volume usage history (in form of a graph and table).

One can configure which of the storage volumes of the given device will be monitored in the Edit Device page, Storage tab.

Services Statistics

The **Services** frame displays the status of monitored network services (e.g., HTTP, FTP, DNS, SMTP, etc.) on the device. To be able to monitor the status of services, the services monitoring must be enabled in the polling profile that is assigned to the given device.

The following icons are used to indicate the current status of services:

- Service is available
- Service is not available

One can configure which of the supported standard services will be monitored in the Edit Device page, Services tab.

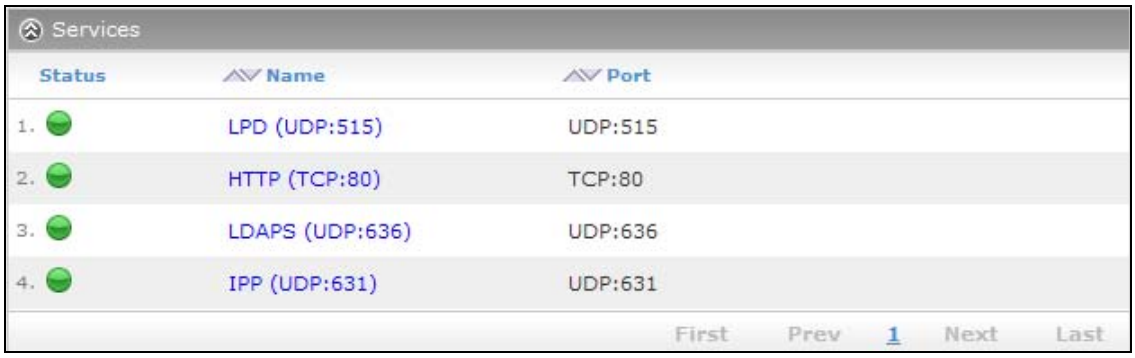


Figure 8: Services frame in the device performance page

By clicking a service in the list, you can view its availability graph and table in a dedicated web page.

Processes Statistics

The **Processes** frame in the device performance web page (Figure 7) displays a list of monitored processes, their current status, path, process identification number (PID), CPU load and memory load for every process.

One can configure which of the processes running on the given device will be monitored in the Edit Device page, Processes tab.

The following icons are used to indicate the current status of processes:

- - Process is running
- - Process is stopped

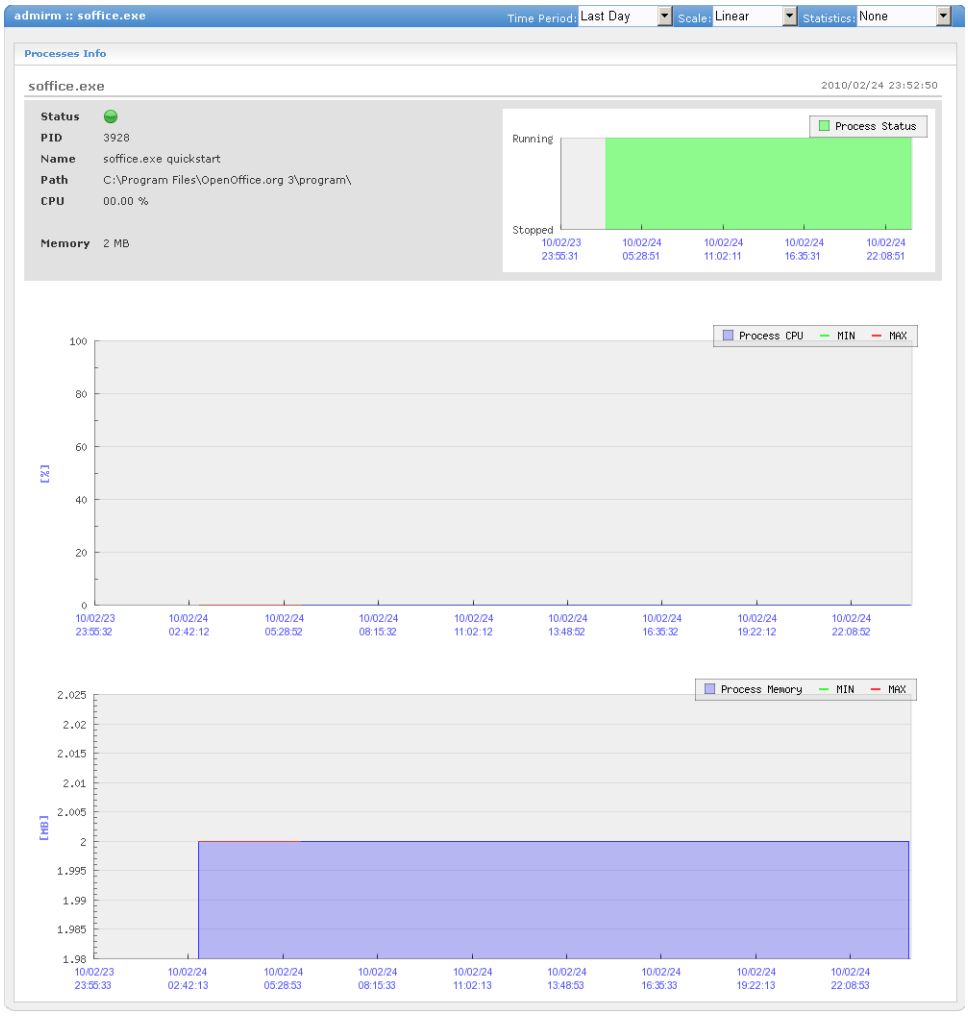


Figure 9: Example of a web page with process statistics

By clicking a process in the list, you can view its detailed statistics in a dedicated web page (Process Info). This includes the graphs for process CPU load and memory consumption.

Network Interfaces Statistics

The **Interfaces** frame of the device performance page displays the lists of monitored network interfaces on the device, as well as the current status, address, type, speed and the inbound and outbound utilization rate for every monitored interface (Figure 7).

One can configure which network interfaces on the given device will be monitored in the Edit Device page, Interfaces tab.

The following icons are used to indicate the current status of interfaces:

- Up – Interface is up
- Down – Interface is down
- Off – Interface has been administratively disabled

By clicking an interface in the list, you can view its detailed statistics in a dedicated web page (Interface Info). This includes the interface utilization rate, bit rate, packet rate, error rate, queue drops (for Cisco devices only) and discard rate statistics with history (Figure 10). Click any tab (Utilization, Bit rate, Error Rate, ..) or graph to view more data for the given metric.

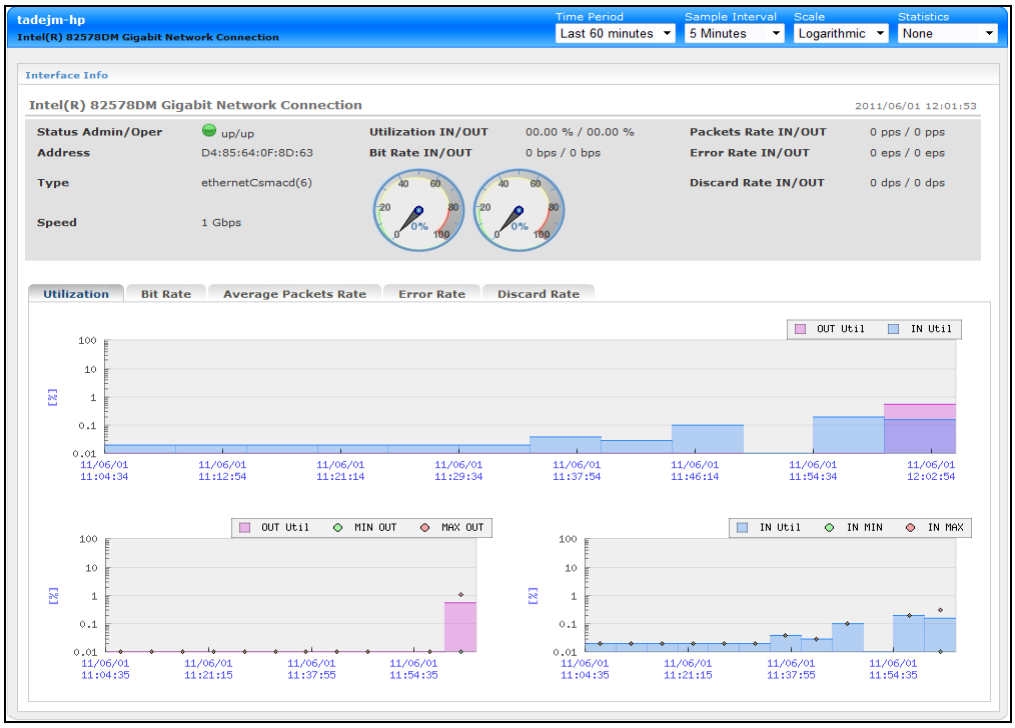


Figure 10: Example of a web page with network interface statistics

IP SLA Statistics

The **IP SLA** frame in the device performance web page (Figure 11) displays the lists of IP SLA categories (e.g., HTTP, DNS, Jitter (VoIP), etc.) and operations within categories (source->destination items) as well as the current IP SLA measurements.

IP SLA statistics can only be monitored on Cisco devices that are properly configured (enabled IP SLA operations), provided that the IP SLA monitoring is enabled in the polling profile assigned to those devices.

For more information on configuring IP SLA operations on Cisco devices, please consult the Cisco documentation
(e.g.: http://www.cisco.com/en/US/docs/ios/12_4/ip_sla/configuration/guide/hsoverv.html).

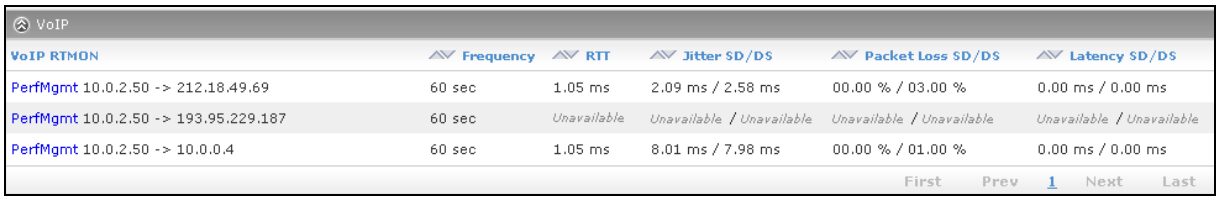


Figure 11: VoIP frame in the device performance page

The **IP SLA** frame in the device performance page displays the lists of IP SLA categories (e.g., HTTP, DNS, Jitter (VoIP), etc.) and operations within categories (source->destination items) configured on the given device. It also displays the current IP SLA measurements, i.e., round trip times (RTT), and for VoIP also jitter from source to destination and vice-versa (Jitter SD/DS), packet loss from source to destination and vice-versa (Packet Loss SD/DS), and latency from source to destination and vice-versa (Latency SD/DS).

By clicking an IP SLA operation in the first column (e.g., VoIP RTTMON), you can view more detailed statistics with history for the given IP SLA operation. For VoIP IP SLA this includes the MOS (mean opinion score), round trip time (RTT), jitter, packet loss, latency, packet out of sequences, packet MIA, and packet late arrivals (Figure 12). For more information about those parameters, please consult the Cisco documentation that came with your equipment.

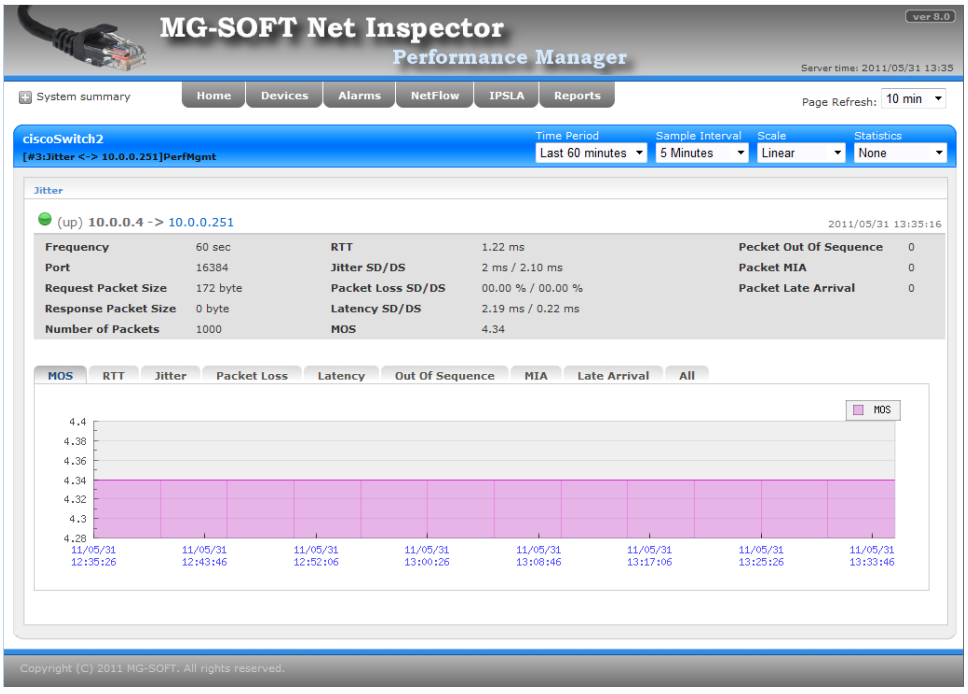


Figure 12: Example of a web page displaying the IP SLA VoIP quality statistics

Device-Related Alarms

The **Alarms** frame in the device performance web page displays all active alarms that are associated with the given device. If no active alarm for the given device exists, the **Alarms** frame is not displayed.

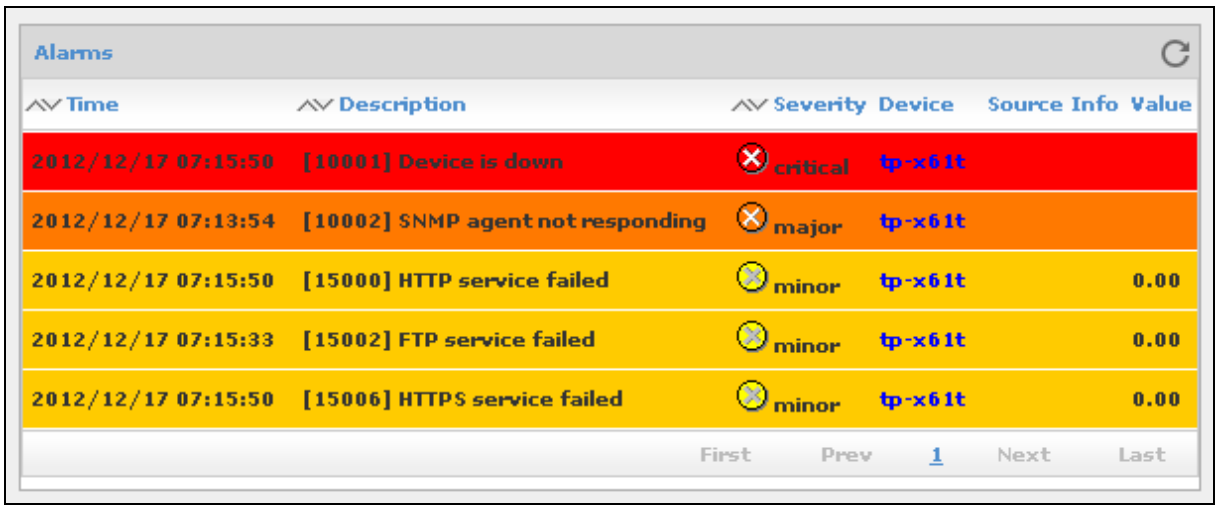


Figure 13: Alarms frame in the device performance page

The following information is displayed for each alarm:

Time	Date and time when the alarm occurred
Description	Short description of the alarm
Severity	Severity of the alarm
Source Info	Additional information about the source of alarm
Value	Value of the variable (for threshold alarms only)

For more information about alarms, please refer to the Viewing Alarms section.

Custom Statistics

The **Custom Statistics** frame (which can be named differently - as defined in the custom polling strategy) in the device performance web page (Figure 7), displays the list of custom (user-configured) SNMP parameters and their values. The **Custom Statistics** frame is not displayed by default. To enable displaying it, enable the **Custom Statistics** category in the Edit Page Layout drop-down frame.

By clicking an item in the list, you can view its detailed statistics in a dedicated web page. This includes a table of retrieved values and a graph of retrieved numerical values of the user-specified SNMP parameters.

3.3.1 Editing Device Performance Page Layout

By default, the device performance page contains frames for all categories of monitored parameters, except the Custom Statistics. Furthermore, the categories (Response time, Memory and Processor Info, Storage Info, Services, etc.) are displayed in 2 columns by default.

The device performance page layout (included frames, order of frames, number of columns) can be customized to meet your preferences. The modified layout can be applied to one device only, to all devices of the same type (e.g., server, router, firewall, etc.) or to all monitored devices in the system.

To Edit the Device Performance Page Layout:

1. Open the device performance page of the device whose page layout you wish to customize by clicking a device name hyperlink on the Devices page.
2. Click the ***Edit page layout*** link below the titlebar of the device performance page (Figure 14).

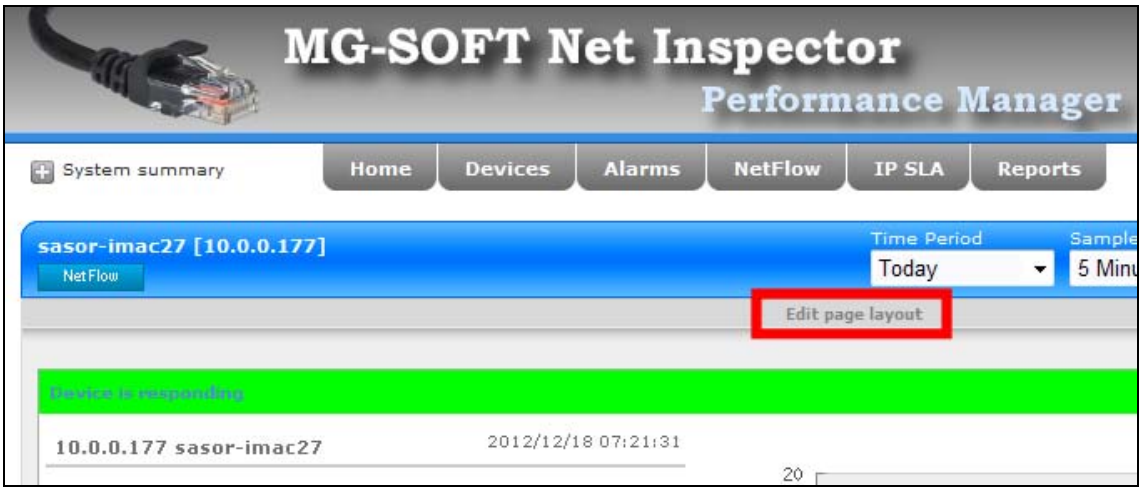


Figure 14: Selecting the Edit page layout link in the device performance page

3. The **Edit Page Layout** drop-down frame opens (Figure 15).

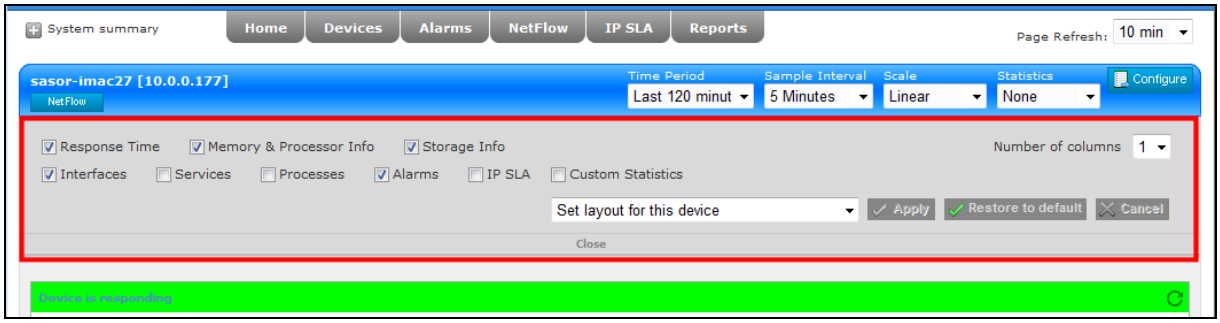


Figure 15: Opened Edit page layout drop-down frame in the device performance page

4. Check the checkboxes in front of the categories to be displayed in the device performance page. The following categories are available:

- Response time
- Memory and Processor Info
- Storage Info
- Interfaces
- Services
- Processes
- IP SLA
- Custom Statistics [named arbitrarily]

5. When you enable a category (check its checkbox), its frame is immediately displayed on the currently opened device performance web page. When you disable a category, its frame immediately disappears from the currently opened device performance page.

> **Note:** An empty frame will be displayed if monitoring of the selected category of parameters is not enabled in the polling profile assigned to the given device or if the device does not return the data from this category.

6. Frames in the device performance page can be displayed in 1, 2 or 3 columns. Select the desired number of columns from the ***Number of columns*** drop-down list in the **Edit Page Layout** drop-down frame (Figure 15).
7. To move a frame to a different location in the device performance page, click the titlebar of the frame, hold down the left mouse button and drag the frame to the desired position. The shaded down-arrow markers appear at the location where the dropped frame will be positioned (Figure 16). Release the left mouse button to drop the frame to the marked position.

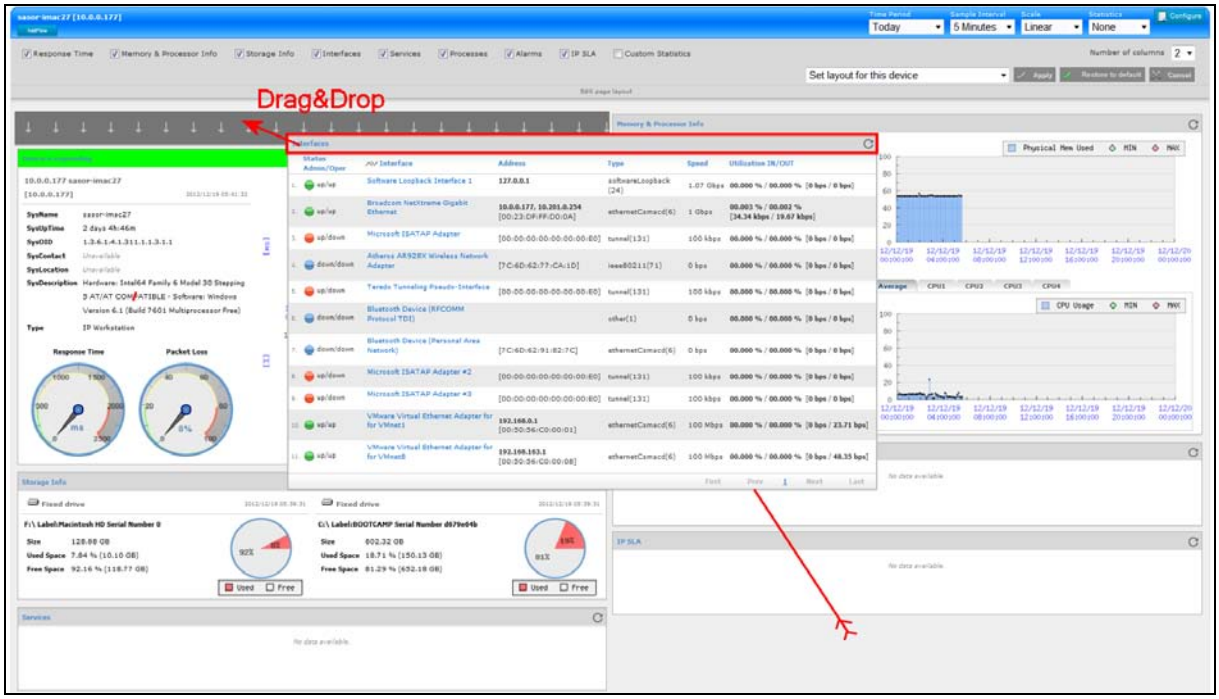


Figure 16: Repositioning a frame using the drag&drop technique

8. When you have finished editing the performance page layout, select the appropriate entry from the **Set layout for…** drop-down list and click the ***Apply*** button next to it to apply the configured layout to the selected device only, to all devices of the same type or to all devices in the system, respectively (Figure 17).

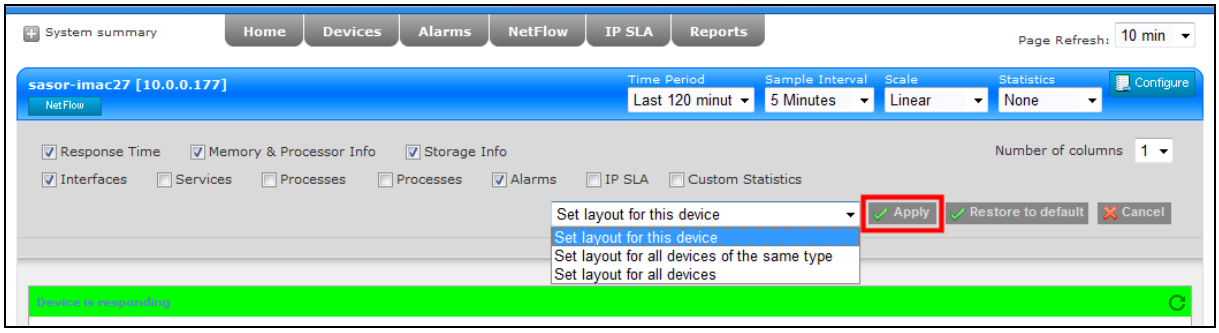


Figure 17: Applying the new page layout to the selected device

9. To close the Edit Page Layout drop-down frame, click the ***Close*** link at the bottom of the Edit Page Layout drop-down frame (Figure 18).

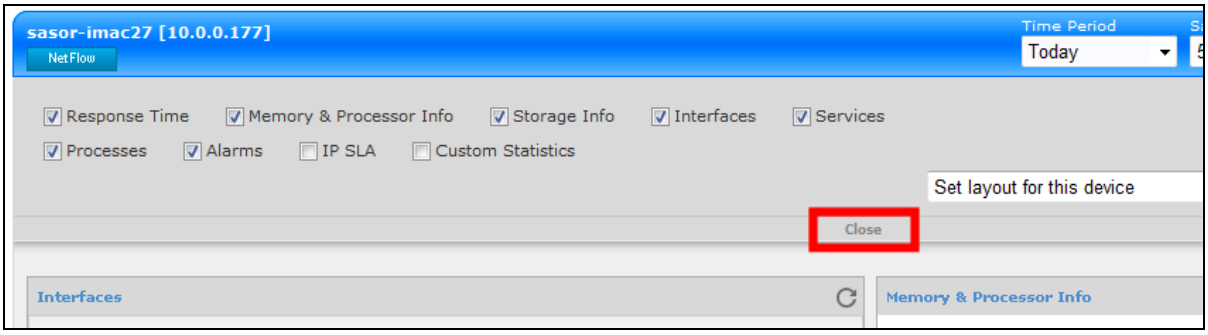


Figure 18: Closing the Edit page layout drop-down frame

To Revert the Device Performance Page Layout to Default Settings:

1. Open the device performance page of the device whose page layout you wish to revert the to default settings.
2. Click the ***Edit page layout*** link below the titlebar of the device performance page (Figure 14). The **Edit Page Layout** drop-down frame opens (Figure 15).
3. Select the appropriate entry from the **Set layout for…** drop-down list and click the ***Restore to default*** button next to it to restore to defaults the page layout of the selected device only, to restore to defaults the page layout for all devices of the same type or to restore to defaults the page layout for all devices in the system, respectively (Figure 17).

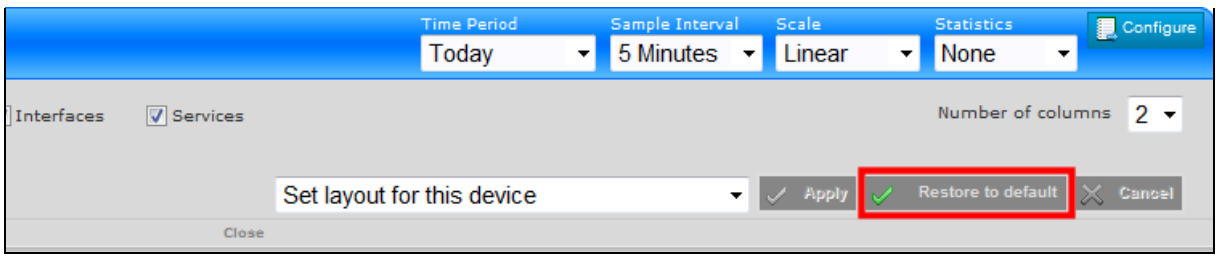


Figure 19: Restoring the page layout to default settings

3.3.2 Configuring Device Monitoring Options (Interfaces, Storage Units, Processes, Services)

By default, all network interfaces, storage units and supported standard network services are automatically monitored for all managed objects (devices). Processes are not monitored by default.

The Edit Device Monitoring Options page lets you configure which interfaces, storage units, services and running processes on the given device will be monitored and which not.

1. To select which interfaces, storage units, processes and services will be monitored for the given device (and thus the corresponding statistics included in the device performance page), click the ***Configure*** button in the upper-right corner of the device performance page titlebar (Figure 20).

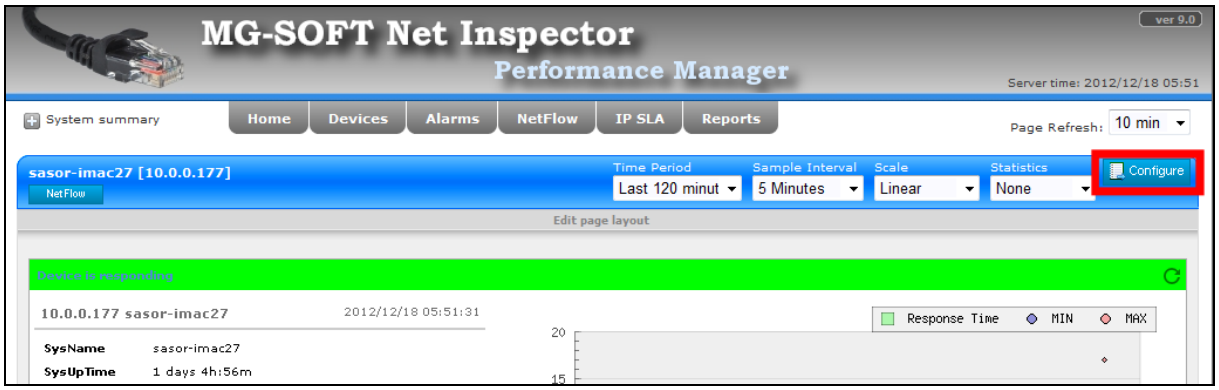


Figure 20: Choosing the Configure button in the device performance page

2. The Edit Device Monitoring Options page is displayed (Figure 21).

3. To enable monitoring one or more network interfaces, click the **Interfaces** tab in the Edit Device Monitoring Options page and check the checkboxes in front of the interfaces you want to be monitored. To disable monitoring a specific interface, uncheck its checkbox in the Interfaces tab. Click the ***Apply*** button at the bottom of the **Interfaces** tab to apply the changes.

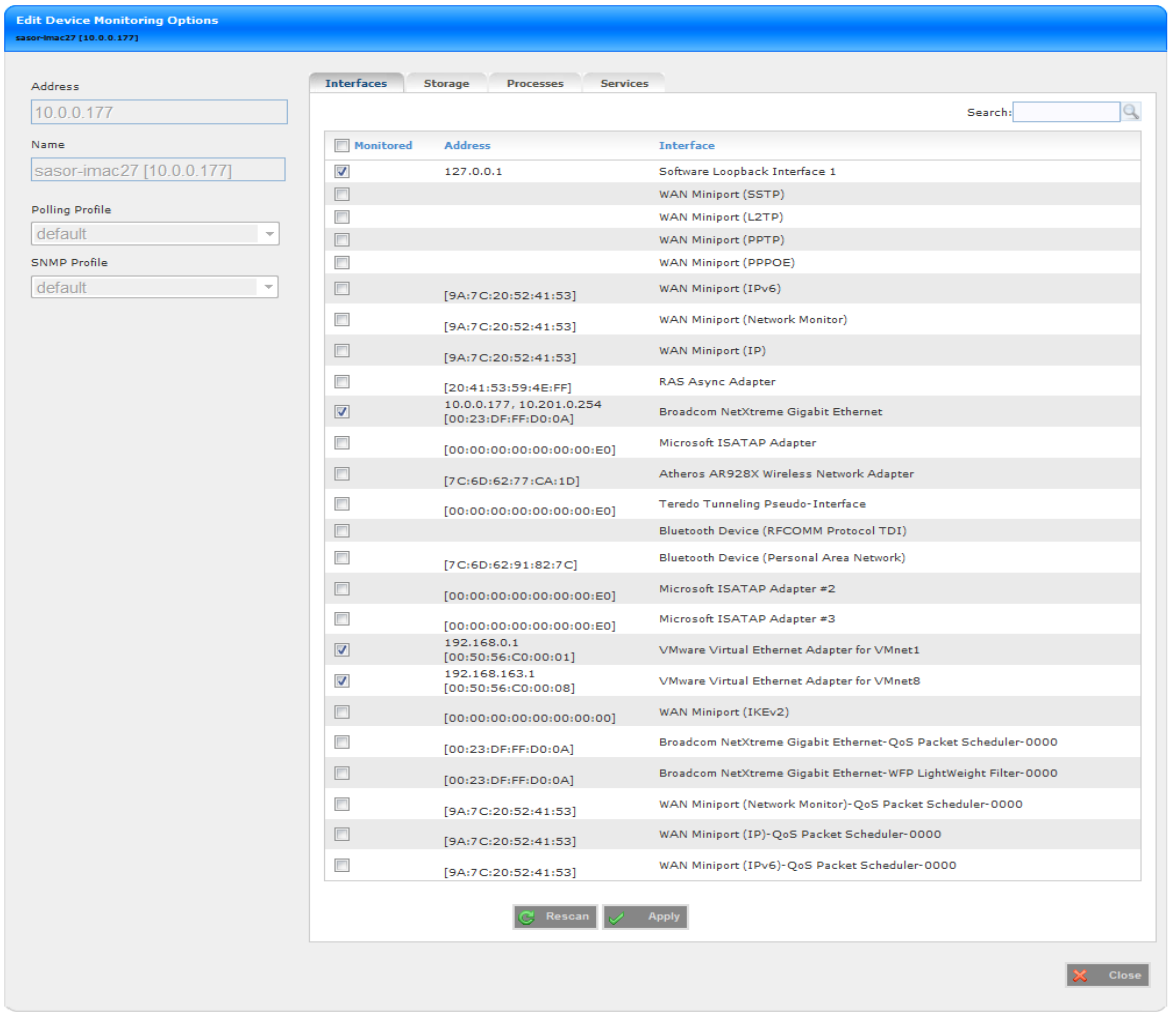


Figure 21: Edit Device Monitoring Options page - Interfaces tab

4. To choose the storage volumes to be monitored, click the **Storage** tab in the Edit Device Monitoring Options Monitoring Options page.

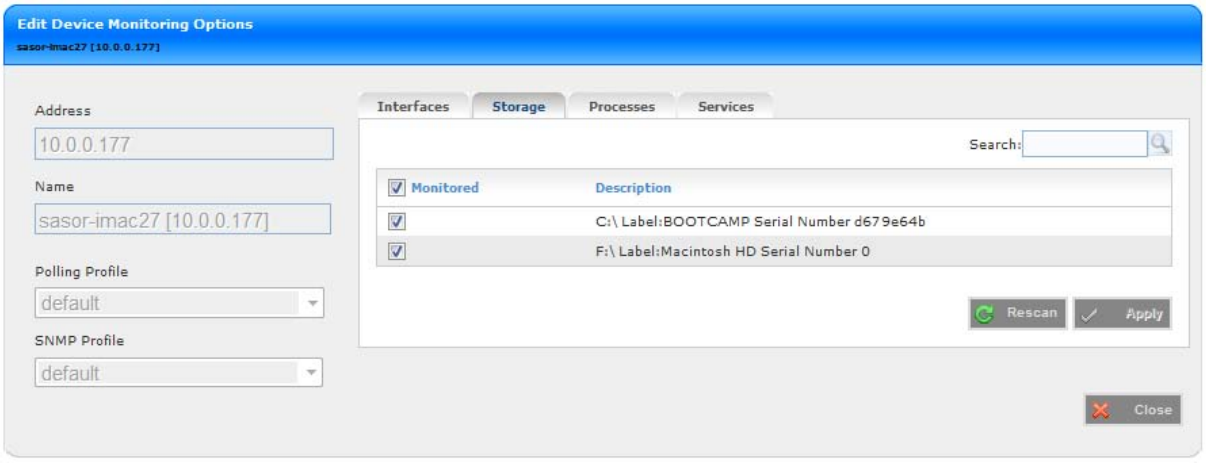


Figure 22: Edit Device Monitoring Options page - Storage tab

5. In the list of storage units in the Storage tab, check the checkboxes of the storage units you want to monitor on the given device, and click the ***Apply*** button.
6. To select the processes you want to monitor on the given device, click on the **Processes** tab.

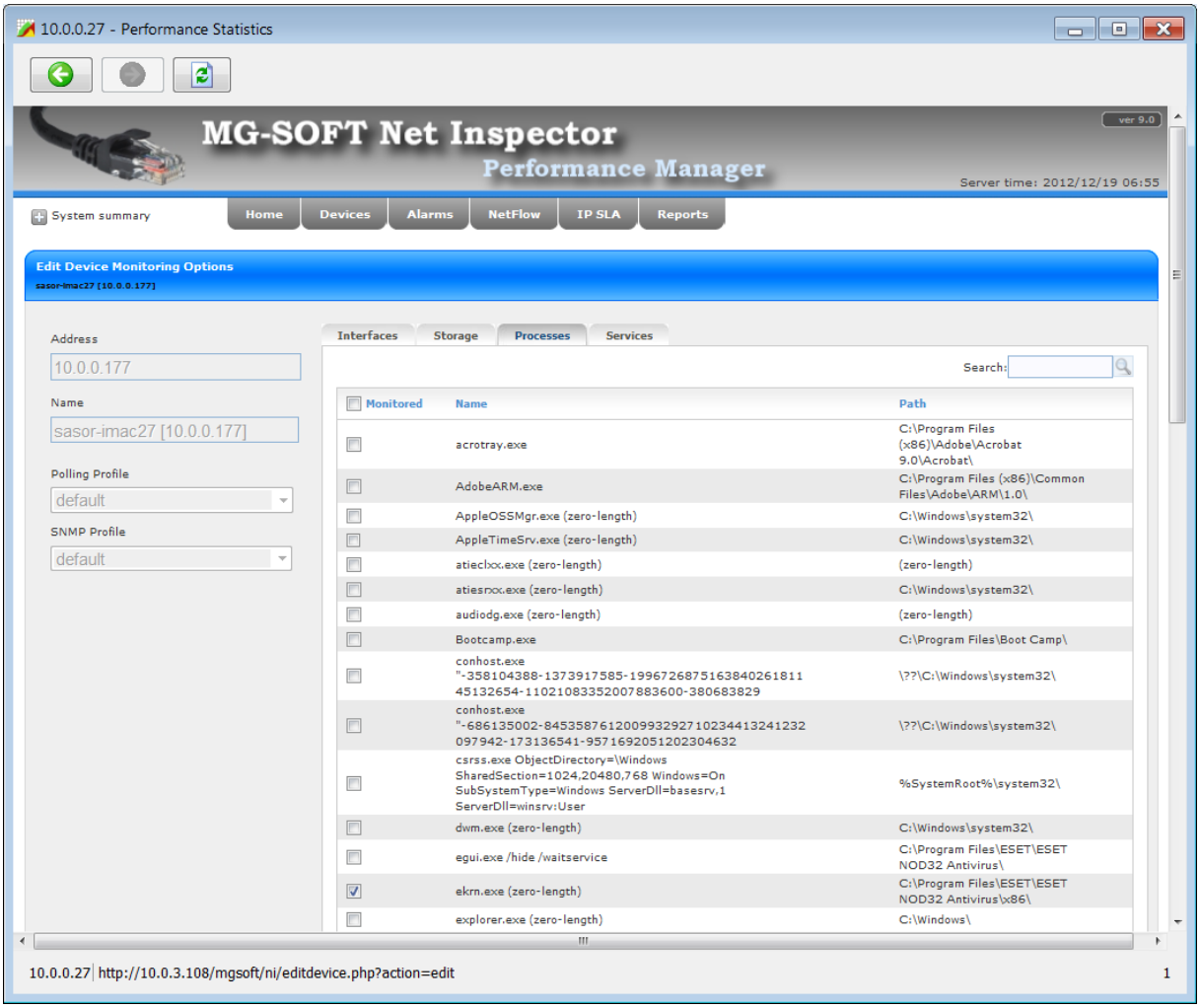


Figure 23: Edit Device Monitoring Options page - Processes tab

7. In the list of processes that run on the given device, check the checkboxes of the processes you want to monitor, and click the ***Apply*** button at the bottom of the Processes list.

8. To choose the network services you want to monitor on that particular device, click on the **Services** tab.

The Services tab lets you scan the well-known ports on the device for supported TCP and UDP network services. These services include HTTP, HTTPS, FTP, DNS, SMTP, IMAP, IMAPS, POP3, SSH, Telnet, NNTP, NNTPS, SIP, H.323, LDAP, LDAPS, IPP, LPD, MsSQL, MySQL and Oracle service. The Services tab lets you configure which of the detected network services will be monitored on the given device. Furthermore, in this view, you can configure to monitor supported services on non-standard ports. Once configured, the device Performance Statistics page displays the status of monitored services (i.e., whether the services are accessible or not).

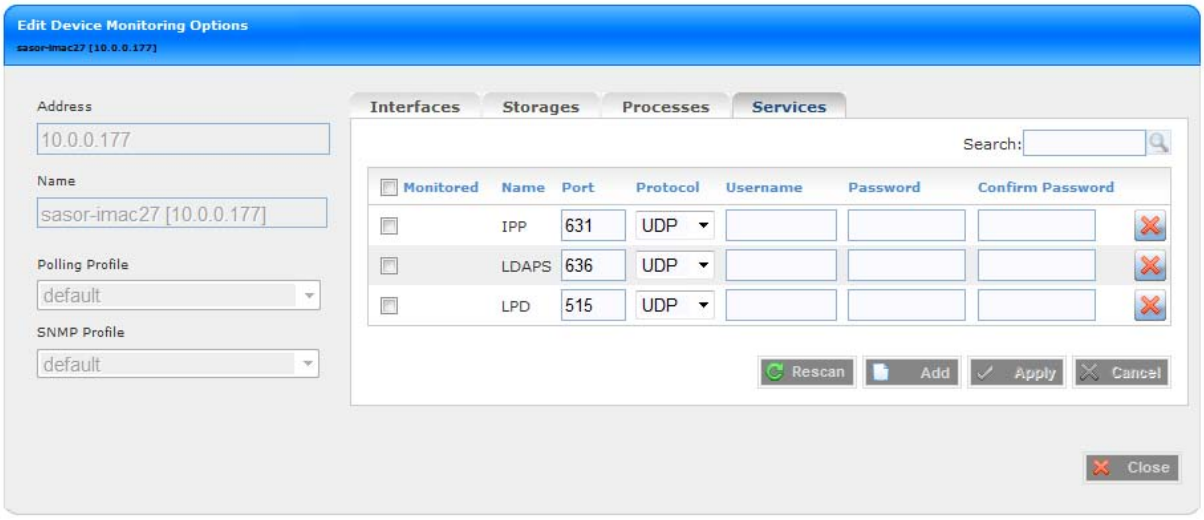


Figure 24: Edit Device Monitoring Options page - Services tab

9. Check the checkboxes in front of the services you want to monitor. If user authentication is required for connecting to a service, enter the **username** and **password** into the accompanying input lines.
10. If there are no services listed, click the ***Rescan*** button to scan the device for supported services. To add a service that is currently not running on that device click the ***Add*** button, and choose the service from the **Name** drop-down list.
11. Click the ***Apply*** button when to apply the changes.
12. To return to the Device Performance Statistics page click the ***Close*** button.

3.4 NetFlow / sFlow Monitoring

Performance Manager in Net Inspector WorkGroup, Enterprise and Carrier Edition incorporates a software NetFlow collector and analyzer module that receive NetFlow v5 and v9 protocol packets and sFlow v5 packets from source devices and provides aggregated statistics about IP traffic (network flows) on NetFlow/sFlow-enabled equipment (like the Cisco IOS devices).

NetFlow is a network protocol for collecting IP traffic information. NetFlow version 9 is documented in RFC 3954.

RFC 3954 defines (network) flow as follows:

A **flow** is defined as a unidirectional sequence of packets with some common properties that pass through a network device. These collected flows are exported to an external device, the NetFlow collector. Network flows are highly granular; for example, flow records include details such as IP addresses, packet and byte counts, timestamps, Type of Service (ToS), application ports, input and output interfaces, etc.

sFlow stands for "sampled flow" and is a method for sampling and exporting truncated packets, together with interface counters. Maintenance of the protocol is performed by the sFlow.org consortium. sFlow v5 (http://sflow.org/sflow_version_5.txt) is supported by Net Inspector.

NetFlow and sFlow monitoring provides insight into how the network is utilized in terms of applications that generate the most traffic (in bytes and packets), it lets you view which endpoints (IP addresses) are the source and destination of the heaviest traffic, what protocols are used most etc. Monitoring IP traffic flows facilitates more accurate capacity planning and ensures that resources are used appropriately in support of organizational goals. It helps IT determine where to apply Quality of Service (QoS), optimize resource usage, etc.

Note 1: To enable NetFlow and/or sFlow monitoring, the source device(s) must be first configured (using a vendor-specific method) to send NetFlow/sFlow packets to Net Inspector NetFlow collector service and the source devices must be set as **NetFlow source** in Net Inspector Client. Please refer to the Net Inspector Installation and Configuration Guide for detailed instructions on how to set a device as a NetFlow source in Net Inspector.

Note 2: Net Inspector Performance Manager displays information received through both, NetFlow and sFlow protocol in the same way. In this section all references to NetFlow apply also to sFlow.

3.4.1 NetFlow Home Page

To open the NetFlow home page (home page) in Net Inspector Client, click the ***Show NetFlow Statistics*** (NF) toolbar button (Figure 25).

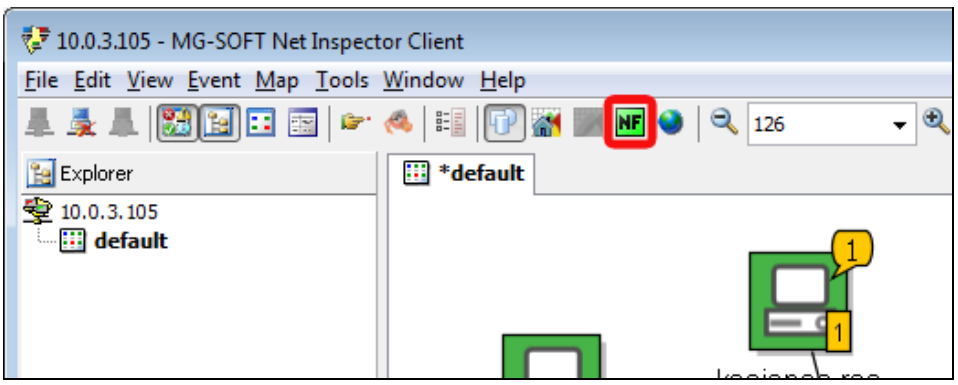


Figure 25: Click the “NF” toolbar button in Net Inspector Client to open the NetFlow home page

Alternatively, if the Performance Manager Home Page is already open in Java web browser, click the ***NetFlow*** tab in the main window (nr. 1 in Figure 26) to view the **NetFlow home page**. The NetFlow home page displays a list of all configured NetFlow / sFlow source devices (if any) and **consolidated Top N** NetFlow traffic reports for a specific (configurable) time frame (e.g., last 60 minutes, today, last 7 days, this month, etc.). The consolidated Top N reports are calculated from all NetFlow sources. The following **Top N** (N is configurable, e.g., 5, 10, 15, 20) NetFlow reports are displayed (a chart and an ordered list is shown in each report):

- Top N Applications: Displays the N applications that transferred the most data;
- Top N Conversations: Displays the N conversations (traffic between two endpoints) that transferred the most data;
- Top N Countries: Displays the top N countries by network traffic.
- Top N Protocols: Displays the top N protocols by network traffic.
- Top N Receivers: Displays the N receivers (hosts) that received the most data.
- Top N Transmitters: Displays the N transmitters (hosts) that sent the most data.
- Top N Transceivers: Displays the N transceivers (hosts) that sent and received the most data.

Note: You can configure the time frame and **N** value for each **Top N** report in the NetFlow configuration page.

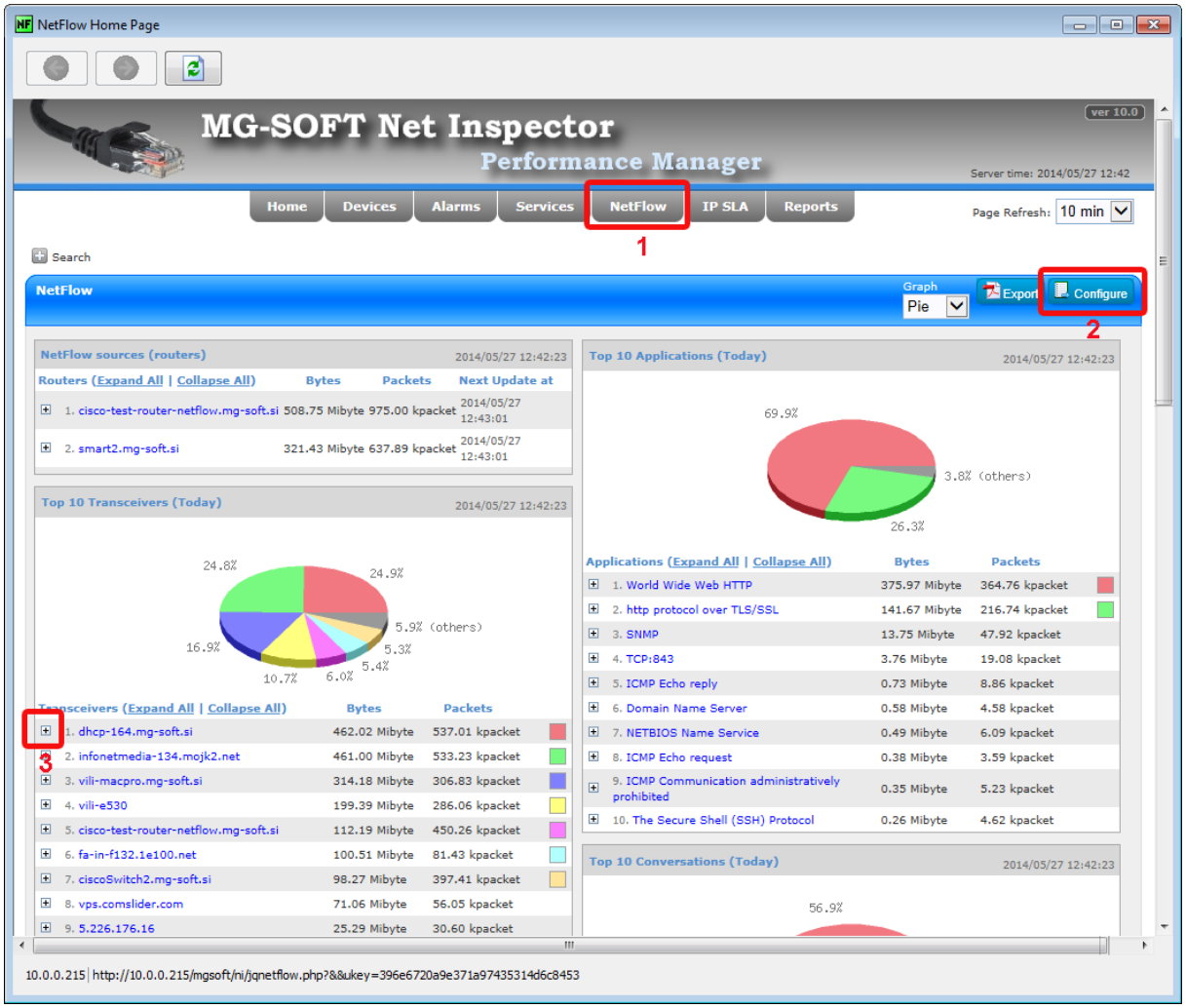


Figure 26: NetFlow home page displays consolidated NetFlow reports

You can choose between two types of charts displayed: a **pie** chart or a **bar** chart. To change the type of charts on a page select the corresponding entry in the ***Graph*** drop-down list (Figure 26).

If you click an item (link) in the NetFlow home page, you will be redirected either to the Router, Interface, Conversation, Application, Country, Protocol or Endpoint Details page with the NetFlow data of the corresponding item (router, interface, conversation, application, country, protocol or endpoint).

By expanding and clicking the individual subentries in the Top N reports, a more detailed statistics for the selected item (e.g., device, interface, conversation, application, etc.) is shown. To view NetFlow/sFlow information of a specific item (e.g., device, interface, conversation, application) on a specific device, click the expand button (⊞) in front of the item you want to examine more closely (nr. 3 in Figure 26) and click on the device name. To see information on the item on a specific interface, click the expand button (⊞) in front of the device you are focusing on and click on the desired interface (Figure 27).

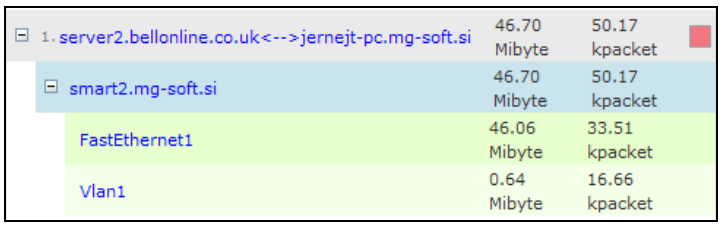


Figure 27: Detailed NetFlow Information

About NetFlow Data Aggregation

Note: NetFlow raw values, 5-minute sum, hourly sum and daily sum

The following model is used for aggregating the NetFlow/sFlow data (note that a different model is used for aggregating the performance data).

How NetFlow data is stored in the database:

* **raw data** as received from NetFlow sources is stored for the **last 24 hours**,
* **5-minute sums** are calculated from raw data and stored for the **last 14 days**,
* **hourly sums** are calculated and stored for the **last 6 months**,
- **daily sums** are calculated and stored for the **last 2 years**.

How NetFlow data is **displayed** in the NetFlow Conversation Details report pages:

Raw data is never depicted in graphs (it is only displayed in tables when viewing the conversation details for up to 24 hours from the current time). In general, the data of the smallest available aggregation level appropriate for the selected time period is displayed, as follows:

1. If the span of the selected time period does not exceed 2 days:
   - 5 min sums are displayed if they are available for the entire period, else
   - hourly sums are displayed if available for the entire period, else
   - daily sums are displayed.

2. If the span of the selected time period exceeds 2 days but does not exceed 2 weeks:
   - hourly sums are displayed if available for the entire period, else
   - daily sums are displayed.

3. If the span of the selected time period exceeds 2 weeks:
   - daily sums are displayed.

Note that you can **zoom into** a graph to view more fine-grained information (if it exists) by selecting a narrower time period in the graph with your mouse.

3.4.2 Router Details Page

To open the ***Router Details Page*** click on the router name in the NetFlow sources section of the **NetFlow home page** (Figure 26).

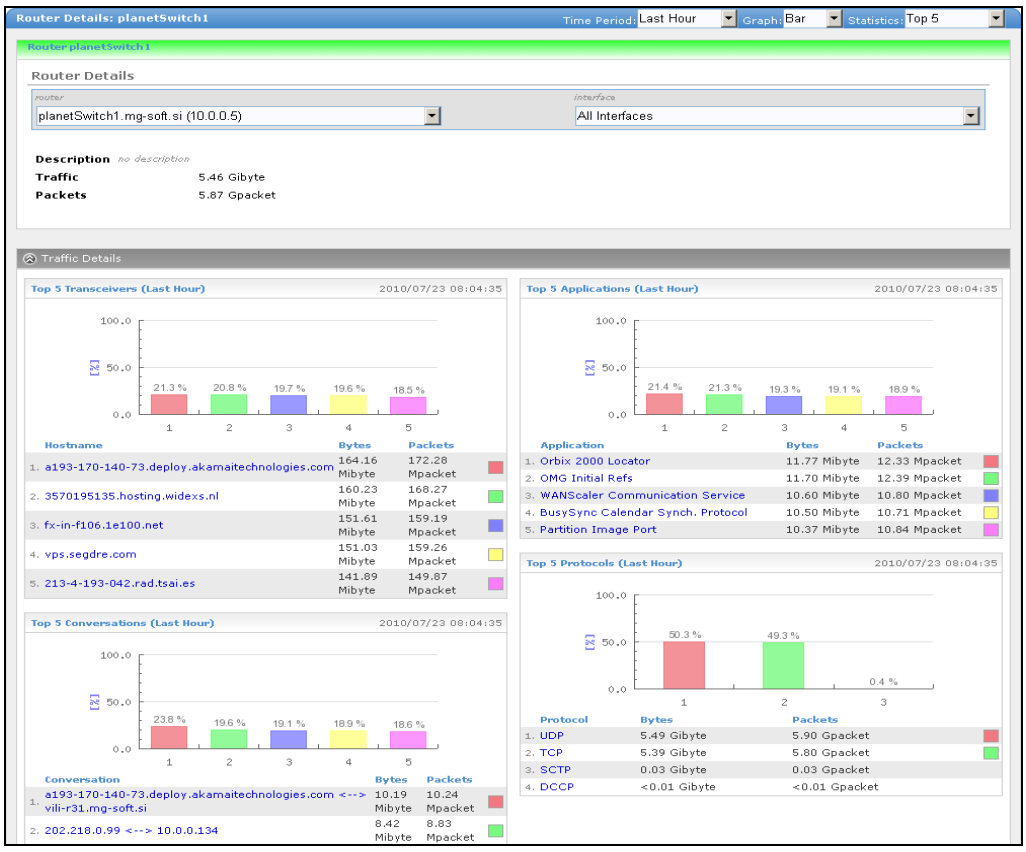

Router Details: planetSwitch1
Time Period: Last Hour
Graph: Bar
Statistics: Top 5
Router planetSwitch1
Router Details
router
planetSwitch1.mg-soft.si (10.0.0.5)
interface
All Interfaces
Description no description
Traffic 5.46 Gibyte
Packets 5.87 Gpacket
Traffic Details
Top 5 Transceivers (Last Hour) 2010/07/23 08:04:35
Hostname Bytes Packets
1. a193-170-140-73.deploy.akamaitechnologies.com 164.16 Mibyte 172.28 Mpacket
2. 3570195135.hosting.widexs.nl 160.23 Mibyte 168.27 Mpacket
3. fx-in-f106.1e100.net 151.61 Mibyte 159.19 Mpacket
4. vps.segdre.com 151.03 Mibyte 159.26 Mpacket
5. 213-4-193-042.rad.tsai.es 141.89 Mibyte 149.87 Mpacket
Top 5 Applications (Last Hour) 2010/07/23 08:04:35
Application Bytes Packets
1. Orbix 2000 Locator 11.77 Mibyte 12.33 Mpacket
2. OMG Initial Refs 11.70 Mibyte 12.39 Mpacket
3. WANScaler Communication Service 10.60 Mibyte 10.80 Mpacket
4. BusySync Calendar Synch. Protocol 10.50 Mibyte 10.71 Mpacket
5. Partition Image Port 10.37 Mibyte 10.84 Mpacket
Top 5 Conversations (Last Hour) 2010/07/23 08:04:35
Conversation Bytes Packets
1. a193-170-140-73.deploy.akamaitechnologies.com <--> vili-r31.mg-soft.si 10.19 Mibyte 10.24 Mpacket
2. 202.218.0.99 <--> 10.0.0.134 8.42 Mibyte 8.83 Mpacket
Top 5 Protocols (Last Hour) 2010/07/23 08:04:35
Protocol Bytes Packets
1. UDP 5.49 Gibyte 5.90 Gpacket
2. TCP 5.39 Gibyte 5.80 Gpacket
3. SCTP 0.03 Gibyte 0.03 Gpacket
4. DCCP <0.01 Gibyte <0.01 Gpacket

Figure 28: Router Details page

On this page, you can see the NetFlow information for the selected router (for all its NetFlow-enabled interfaces). If you want to see data for a specific interface on the router, select if from the interfaces drop-down list and you will be redirected to the ***Interface Details Page***. The following reports are displayed on the **Router Details Page**:

- Top N Transceivers,
- Top N Applications,
- Top N Conversations,
- Top N Protocols and
- Top N Countries.

Note: in the upper right corner of the frame, you can select the **time period, graph** (bar or pie), **and the N** value for all **Top N** reports displayed in this page.

If you click on the name of an item, you will be redirected to the corresponding page (Endpoint Details page if the item is a transceiver, Application Details page if the item is an application, etc.) displaying information related to that item on a given router.

3.4.3 Interface Details Page

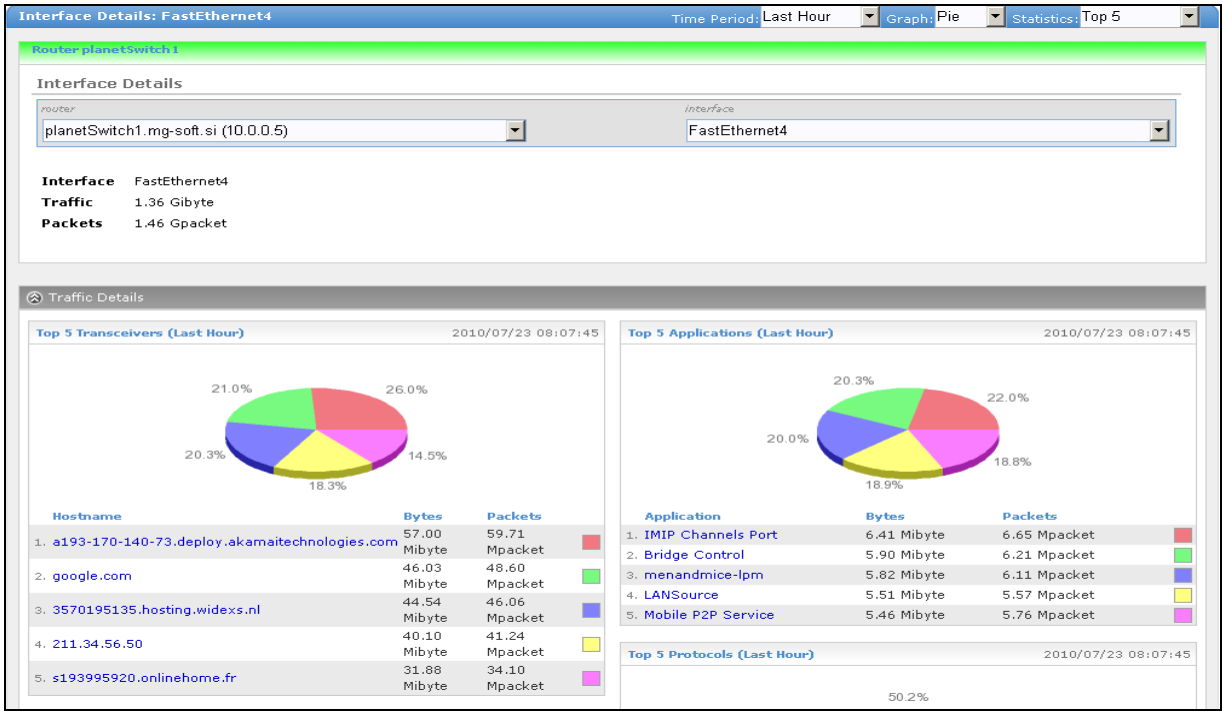


Figure 29: Interface Details page

To open the ***Interface Details Page*** click the expand button (⊞) in front of the device (e.g., router) in the **NetFlow home page** (Figure 26), to show the list of monitored interfaces, then click the name of the interface whose traffic you want to view or select the interface from the drop-down list in the ***Router Details Page*** (Figure 28).

On this page, you can monitor the traffic information of a specific network interface. The information is split into several different groups:

- Top N Transceivers,
- Top N Applications,
- Top N Conversations,
- Top N Protocols and
- Top N Countries.

Note: in the upper right corner of the frame, you can select the **time period, graph** (bar or pie), **and the N** value for all **Top N** reports displayed in this page.

If you click on the name of an item, you will be redirected to the appropriate page (Endpoint Details page if the item is a transceiver, Application Details page if the item is an application, etc.) displaying information related to that item on a specific router.

3.4.4 Conversation Details Page

To view the ***Conversation Details*** page click the conversation whose details you want to view in the Top N Conversations report.

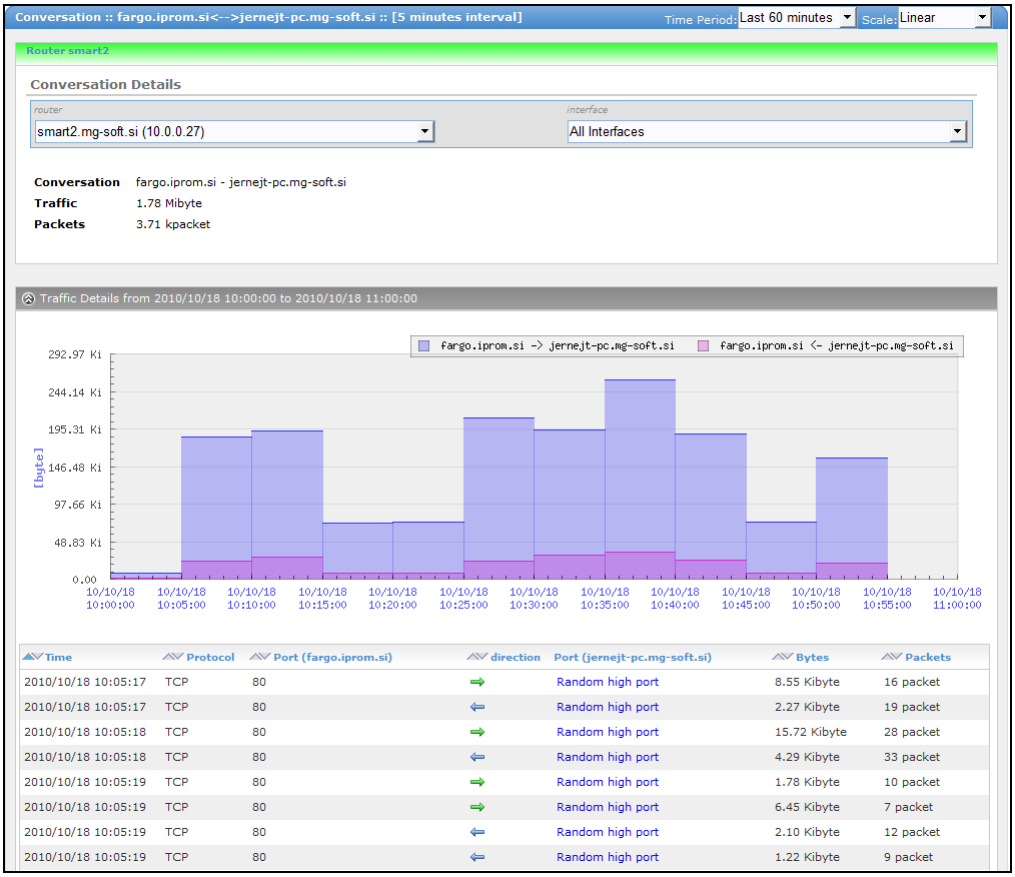

Conversation :: fargo.iprom.si<-->jernejt-pc.mg-soft.si :: [5 minutes interval]
Time Period: Last 60 minutes
Scale: Linear
Router smart2
Conversation Details
router
smart2.mg-soft.si (10.0.0.27)
interface
All Interfaces
Conversation fargo.iprom.si - jernejt-pc.mg-soft.si
Traffic 1.78 Mibyte
Packets 3.71 kpacket
Traffic Details from 2010/10/18 10:00:00 to 2010/10/18 11:00:00
fargo.iprom.si -> jernejt-pc.mg-soft.si
fargo.iprom.si <- jernejt-pc.mg-soft.si
[byte]
292.97 Ki
244.14 Ki
195.31 Ki
146.48 Ki
97.66 Ki
48.83 Ki
0.00
10/10/18 10:00:00
10/10/18 10:05:00
10/10/18 10:10:00
10/10/18 10:15:00
10/10/18 10:20:00
10/10/18 10:25:00
10/10/18 10:30:00
10/10/18 10:35:00
10/10/18 10:40:00
10/10/18 10:45:00
10/10/18 10:50:00
10/10/18 10:55:00
10/10/18 11:00:00
Time Protocol Port (fargo.iprom.si) direction Port (jernejt-pc.mg-soft.si) Bytes Packets
2010/10/18 10:05:17 TCP 80 Random high port 8.55 Kibyte 16 packet
2010/10/18 10:05:17 TCP 80 Random high port 2.27 Kibyte 19 packet
2010/10/18 10:05:18 TCP 80 Random high port 15.72 Kibyte 28 packet
2010/10/18 10:05:18 TCP 80 Random high port 4.29 Kibyte 33 packet
2010/10/18 10:05:19 TCP 80 Random high port 1.78 Kibyte 10 packet
2010/10/18 10:05:19 TCP 80 Random high port 6.45 Kibyte 7 packet
2010/10/18 10:05:19 TCP 80 Random high port 2.10 Kibyte 12 packet
2010/10/18 10:05:19 TCP 80 Random high port 1.22 Kibyte 9 packet

Figure 30: Conversation Details page

In the ***Conversation Details*** page, you can view the traffic details of the conversation visually (in a bar graph) and numerically (in a table). You can monitor the information on all interfaces of the selected router or choose the router or interface you want to focus on in the ***Router*** or ***Interface*** drop-down list.

Note: You can configure the **time period** and the **scale** in the upper right corner of the page.

For the last 24 hours period the raw data, i.e., individual flows as received from the NetFlow source, are displayed in the table below the graph. A flow is a unidirectional sequence of packets passed from one endpoint (IP address and port) to another. One can view the history and direction of flows of the selected conversation in terms of bytes and packets transferred.

The graph always displays aggregated NetFlow data. For example, if the selected time period does not exceed 2 days (for example, if you select “This hour”, “Last 60 minutes”, “Last hour”, “Last 120 minutes”, “Today”, or “Yesterday” option from the ***Time period*** drop-down list), the graph displays 5-minute sum bars. The 5-minute sum bars show how many bytes* has been transferred in each direction between two endpoints in 5 minute intervals spread over the selected time frame.

* Or kibibytes (=2^{10} bytes), or mebibytes (=2^{20} bytes), or gibibytes (=2^{30} bytes), etc.

Click on the graph to view a larger conversation details graph. You can quickly adjust the time period by selecting it from the ***Adjust Time Period*** drop-down list located

below the graph. You can also select the **Custom** option from this drop-down list and specify the Beginning time and End time for the graph in the accompanying drop-down lists. Alternatively, you can **quickly zoom-in** by selecting the desired time period with your mouse (Figure 31).

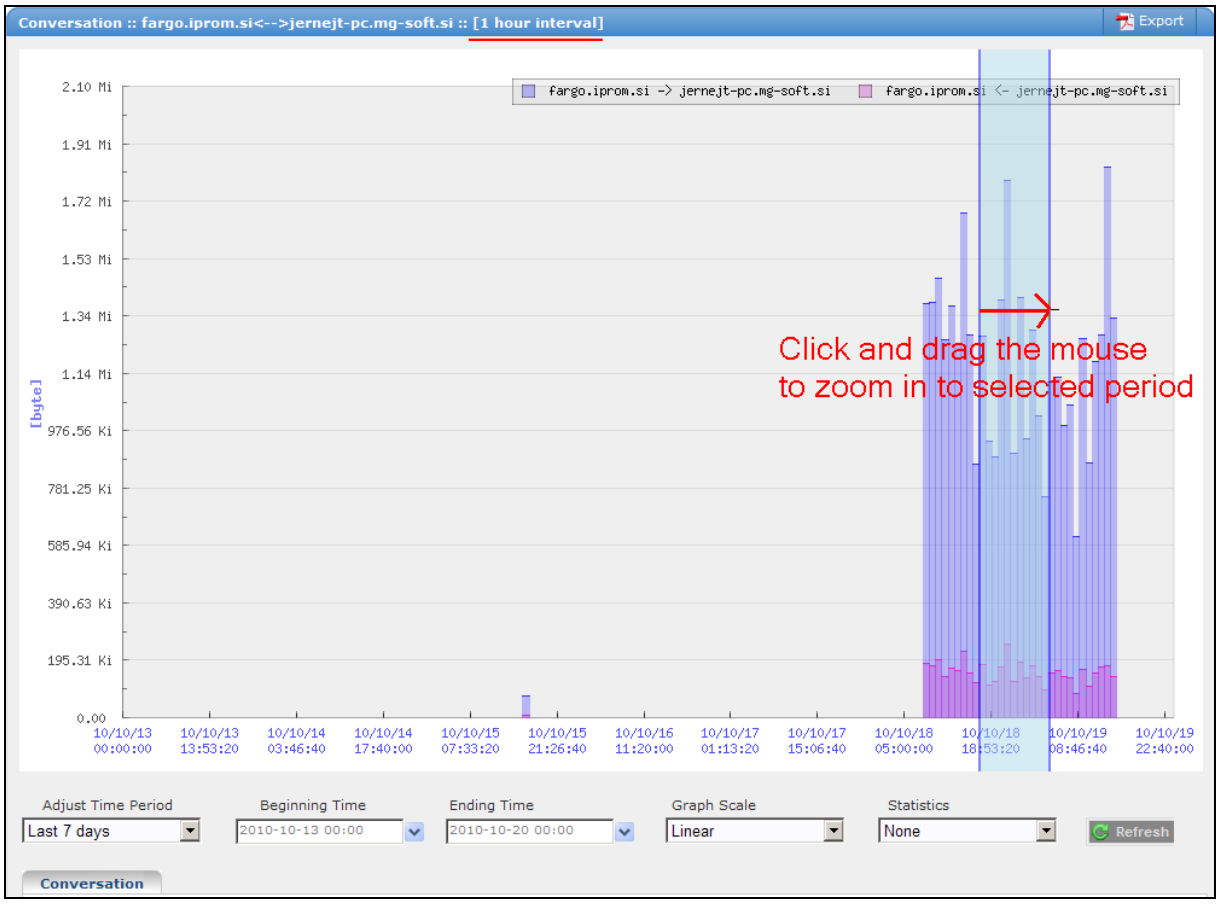


Figure 31: Zooming in the conversation details graph

After zooming-in, a new graph for the selected time period is displayed and the aggregation level of data automatically changes to show more fine-grained information, e.g. from 1 hour sums to 5 minute sums (Figure 32).

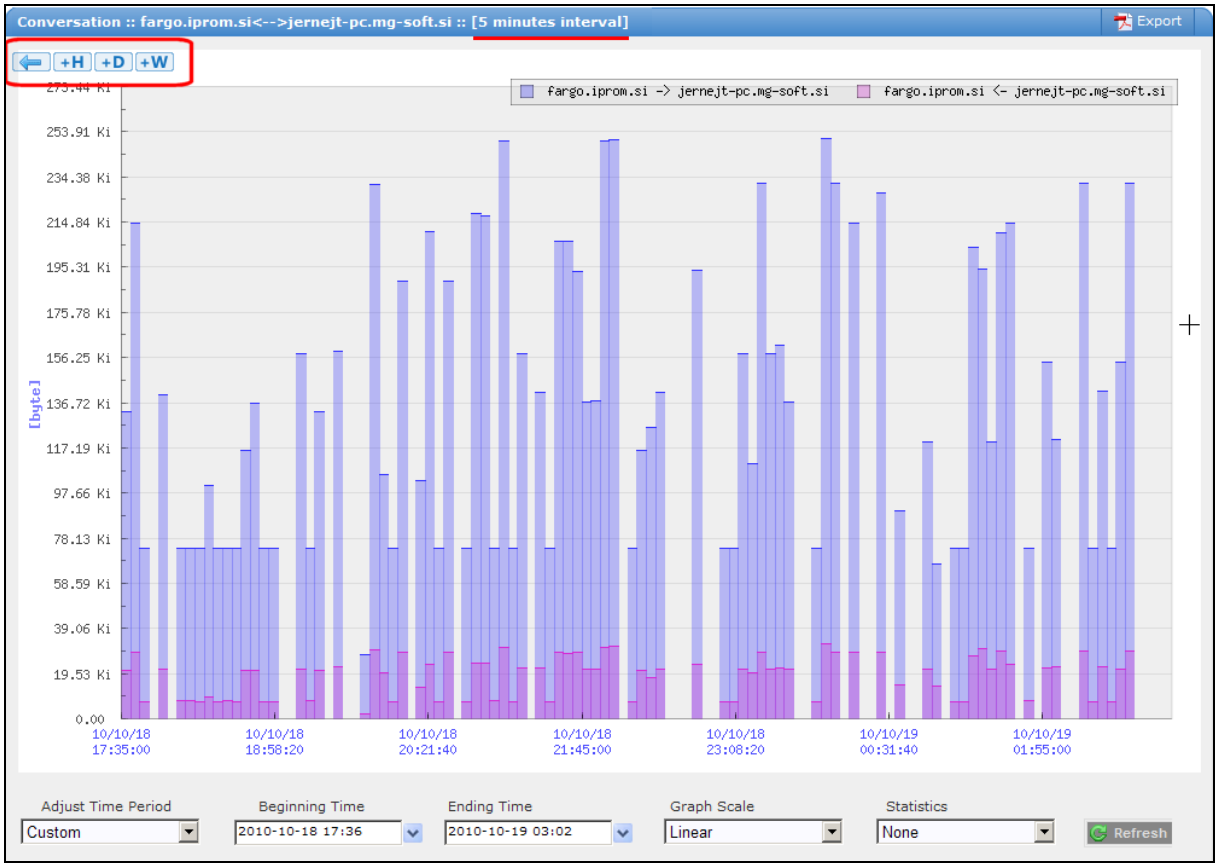


Figure 32: Zoomed in conversation details graph (note the 5 min aggregation level of data)

You can quickly return to the previous zoom level by clicking the button in the upper-left section of the frame (Figure 32).

You can quickly extend the x-axis to the left to include an additional hour, day or week by clicking the +H, +D, or +W button, respectively.

3.4.5 Endpoint Details Page

To view the ***Endpoint Details Page*** for a specific endpoint host, click its name in the lists of Top N transceivers, receivers or transmitters in the NetFlow home page.

Here you can monitor the traffic information of the chosen endpoint. The information is split in different groups:

- Top N Conversations,
- Top N Applications,
- Top N Endpoints Received from
- Top N Endpoints Transmitted to,
- Top N Countries Received from,
- Top N Countries Transmitted to,
- Top N Protocols.

Note: in the upper right corner of the frame, you can select the **time period, graph** (bar or pie), **and the N** value for all **Top N** reports displayed in this page.

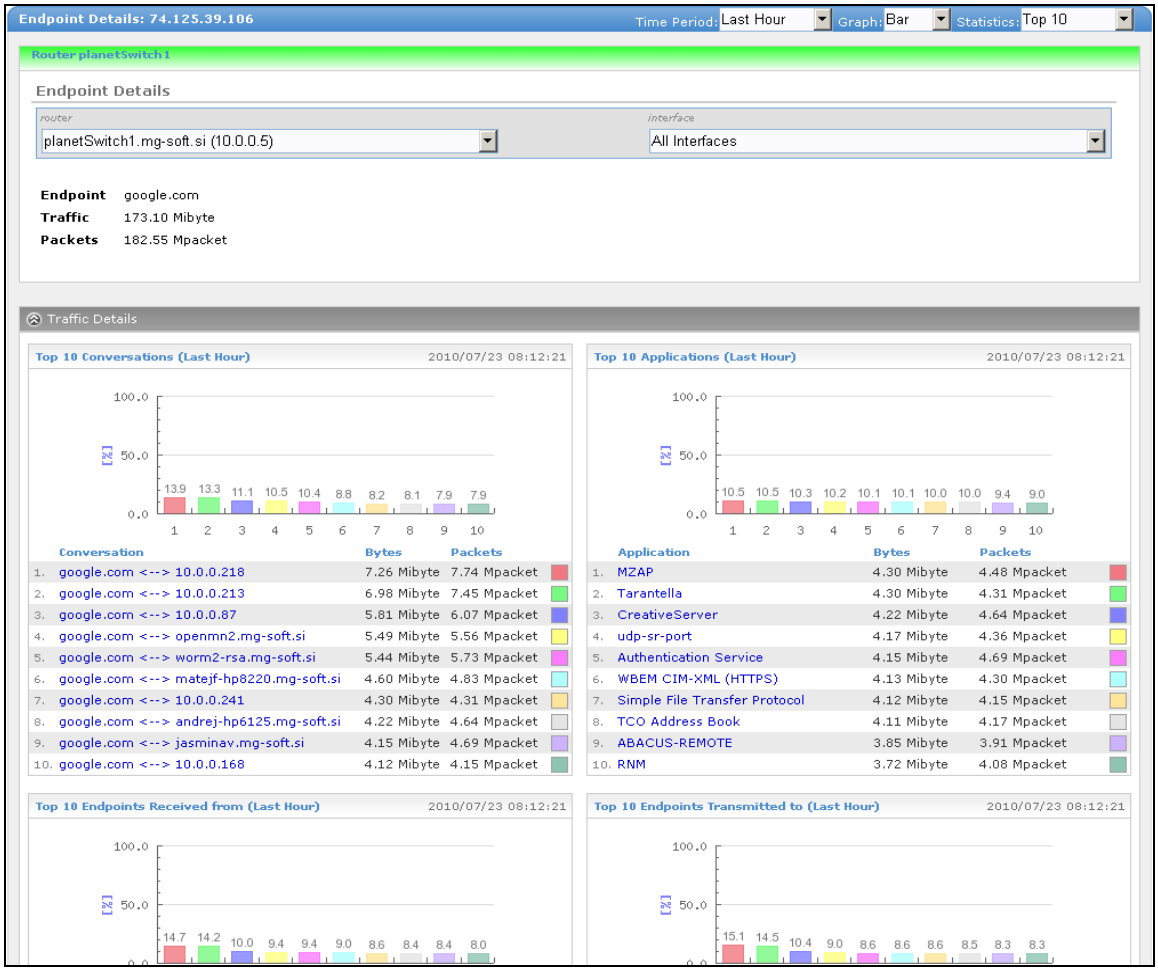

Endpoint Details: 74.125.39.106
Time Period: Last Hour
Graph: Bar
Statistics: Top 10
Router planetSwitch1
Endpoint Details
router
planetSwitch1.mg-soft.si (10.0.0.5)
interface
All Interfaces
Endpoint google.com
Traffic 173.10 Mibyte
Packets 182.55 Mpacket
Traffic Details
Top 10 Conversations (Last Hour) 2010/07/23 08:12:21
Conversation Bytes Packets
1. google.com <--> 10.0.0.218 7.26 Mibyte 7.74 Mpacket
2. google.com <--> 10.0.0.213 6.98 Mibyte 7.45 Mpacket
3. google.com <--> 10.0.0.87 5.81 Mibyte 6.07 Mpacket
4. google.com <--> openmn2.mg-soft.si 5.49 Mibyte 5.56 Mpacket
5. google.com <--> worm2-rsa.mg-soft.si 5.44 Mibyte 5.73 Mpacket
6. google.com <--> matejf-hp8220.mg-soft.si 4.60 Mibyte 4.83 Mpacket
7. google.com <--> 10.0.0.241 4.30 Mibyte 4.31 Mpacket
8. google.com <--> andrej-hp6125.mg-soft.si 4.22 Mibyte 4.64 Mpacket
9. google.com <--> jasminav.mg-soft.si 4.15 Mibyte 4.69 Mpacket
10. google.com <--> 10.0.0.168 4.12 Mibyte 4.15 Mpacket
Top 10 Applications (Last Hour) 2010/07/23 08:12:21
Application Bytes Packets
1. MZAP 4.30 Mibyte 4.48 Mpacket
2. Tarantella 4.30 Mibyte 4.31 Mpacket
3. CreativeServer 4.22 Mibyte 4.64 Mpacket
4. udp-sr-port 4.17 Mibyte 4.36 Mpacket
5. Authentication Service 4.15 Mibyte 4.69 Mpacket
6. WBEM CIM-XML (HTTPS) 4.13 Mibyte 4.30 Mpacket
7. Simple File Transfer Protocol 4.12 Mibyte 4.15 Mpacket
8. TCO Address Book 4.11 Mibyte 4.17 Mpacket
9. ABACUS-REMOTE 3.85 Mibyte 3.91 Mpacket
10. RNM 3.72 Mibyte 4.08 Mpacket
Top 10 Endpoints Received from (Last Hour) 2010/07/23 08:12:21
Top 10 Endpoints Transmitted to (Last Hour) 2010/07/23 08:12:21

Figure 33: Endpoint Details page

If you click on the name of an item, you will be redirected to the corresponding page (Endpoint Details page if the item is an endpoint, Application Details page if the item is an application, etc.) displaying information related to that specific item on a specific router.

3.4.6 Protocol Details Page

To monitor the net flow information sorted by protocol click a protocol name in the home page.

Here you can monitor the traffic information sorted by a specific protocol. The information is split in different groups:

- Top N Conversations,
- Top N Applications,
- Top N Transmitters,
- Top N Receivers,
- Top N Transceivers,
- Top N Transmitting Countries,
- Top N Receiving Countries.

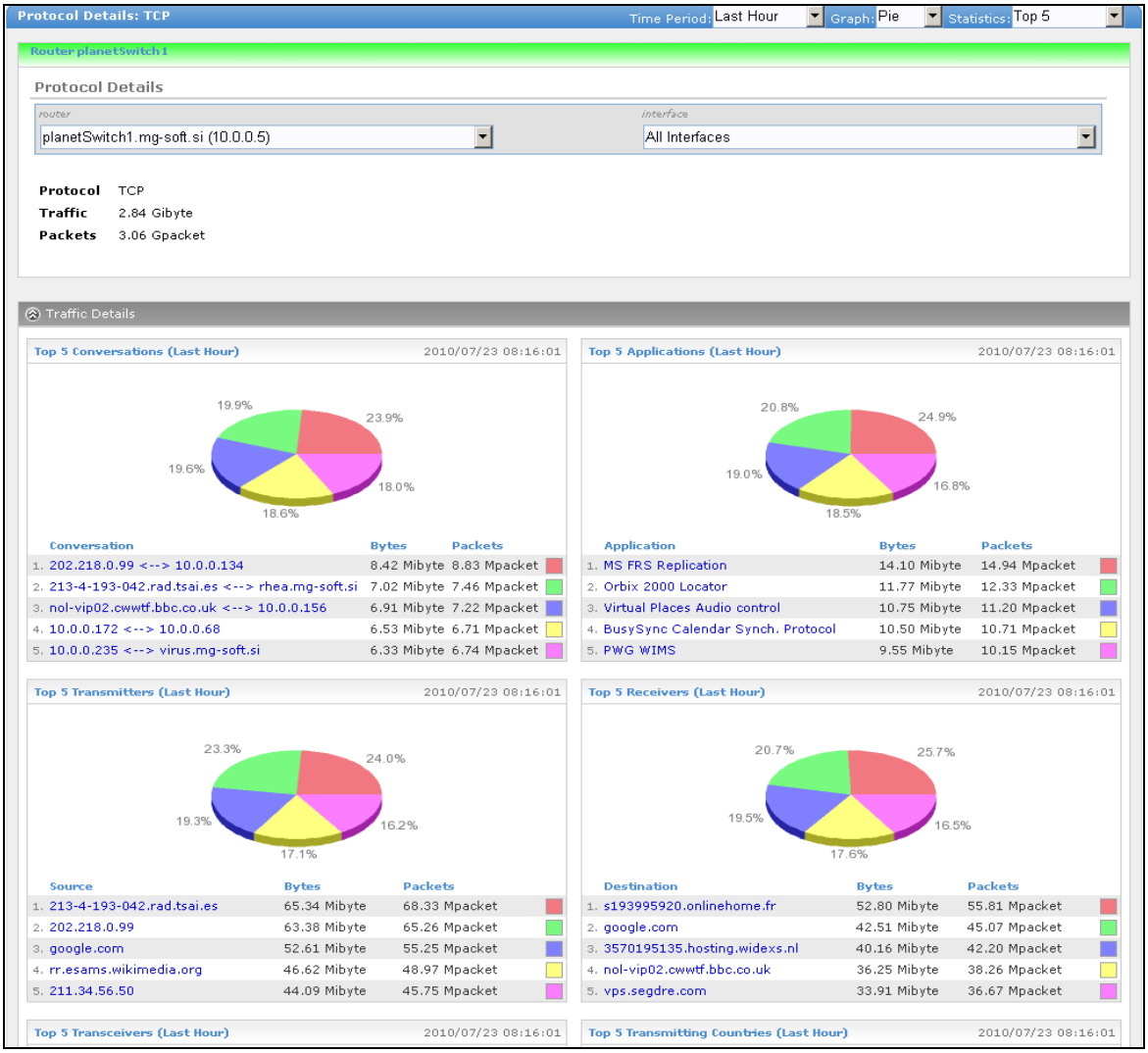

Protocol Details: TCP
Time Period: Last Hour
Graph: Pie
Statistics: Top 5
Router planetSwitch1
Protocol Details
router
planetSwitch1.mg-soft.si (10.0.0.5)
interface
All Interfaces
Protocol TCP
Traffic 2.84 Gibyte
Packets 3.06 Gpacket
Traffic Details
Top 5 Conversations (Last Hour) 2010/07/23 08:16:01
19.9% 23.9% 19.6% 18.0% 18.6%
Conversation Bytes Packets
1. 202.218.0.99 <--> 10.0.0.134 8.42 Mibyte 8.83 Mpacket
2. 213-4-193-042.rad.tsai.es <--> rhea.mg-soft.si 7.02 Mibyte 7.46 Mpacket
3. nol-vip02.cwwtf.bbc.co.uk <--> 10.0.0.156 6.91 Mibyte 7.22 Mpacket
4. 10.0.0.172 <--> 10.0.0.68 6.53 Mibyte 6.71 Mpacket
5. 10.0.0.235 <--> virus.mg-soft.si 6.33 Mibyte 6.74 Mpacket
Top 5 Applications (Last Hour) 2010/07/23 08:16:01
20.8% 24.9% 19.0% 16.8% 18.5%
Application Bytes Packets
1. MS FRS Replication 14.10 Mibyte 14.94 Mpacket
2. Orbix 2000 Locator 11.77 Mibyte 12.33 Mpacket
3. Virtual Places Audio control 10.75 Mibyte 11.20 Mpacket
4. BusySync Calendar Synch. Protocol 10.50 Mibyte 10.71 Mpacket
5. PWG WIMS 9.55 Mibyte 10.15 Mpacket
Top 5 Transmitters (Last Hour) 2010/07/23 08:16:01
23.3% 24.0% 19.3% 16.2% 17.1%
Source Bytes Packets
1. 213-4-193-042.rad.tsai.es 65.34 Mibyte 68.33 Mpacket
2. 202.218.0.99 63.38 Mibyte 65.26 Mpacket
3. google.com 52.61 Mibyte 55.25 Mpacket
4. rr.esams.wikimedia.org 46.62 Mibyte 48.97 Mpacket
5. 211.34.56.50 44.09 Mibyte 45.75 Mpacket
Top 5 Receivers (Last Hour) 2010/07/23 08:16:01
20.7% 25.7% 19.5% 16.5% 17.6%
Destination Bytes Packets
1. s193995920.onlinehome.fr 52.80 Mibyte 55.81 Mpacket
2. google.com 42.51 Mibyte 45.07 Mpacket
3. 3570195135.hosting.widexs.nl 40.16 Mibyte 42.20 Mpacket
4. nol-vip02.cwwtf.bbc.co.uk 36.25 Mibyte 38.26 Mpacket
5. vps.segdre.com 33.91 Mibyte 36.67 Mpacket
Top 5 Transceivers (Last Hour) 2010/07/23 08:16:01
Top 5 Transmitting Countries (Last Hour) 2010/07/23 08:16:01

Figure 34: Protocol Details page

> **Note:** in the upper right corner of the frame, you can select the **time period, graph** (bar or pie), **and the N** value for all **Top N** reports displayed in this page.

When you click on the name of an item, you are redirected to the appropriate page (Endpoint Details page if the item is a receiver, Application Details page if the item is an application, etc.) displaying information related to that specific item on a specific router.

3.4.7 Country Details Page

To open the ***Country Details page*** click a country you want to view the IP traffic details of in the home page.

On this page you can monitor:

- Top N Endpoints Received From,
- Top N Endpoints Transmitted To,
- Top N Transceivers,
- Top N Protocols,
- Top N Applications,
- Top N Conversations.

Note: in the upper right corner of the frame, you can select the **time period, graph** (bar or pie), **and the N** value for all **Top N** reports displayed in this page.

If you click on the name of an item, you will be redirected to the appropriate page (Endpoint Details page if the item is an endpoint, Application Details page if the item is an application, etc.) displaying information related to that specific item on a specific router.

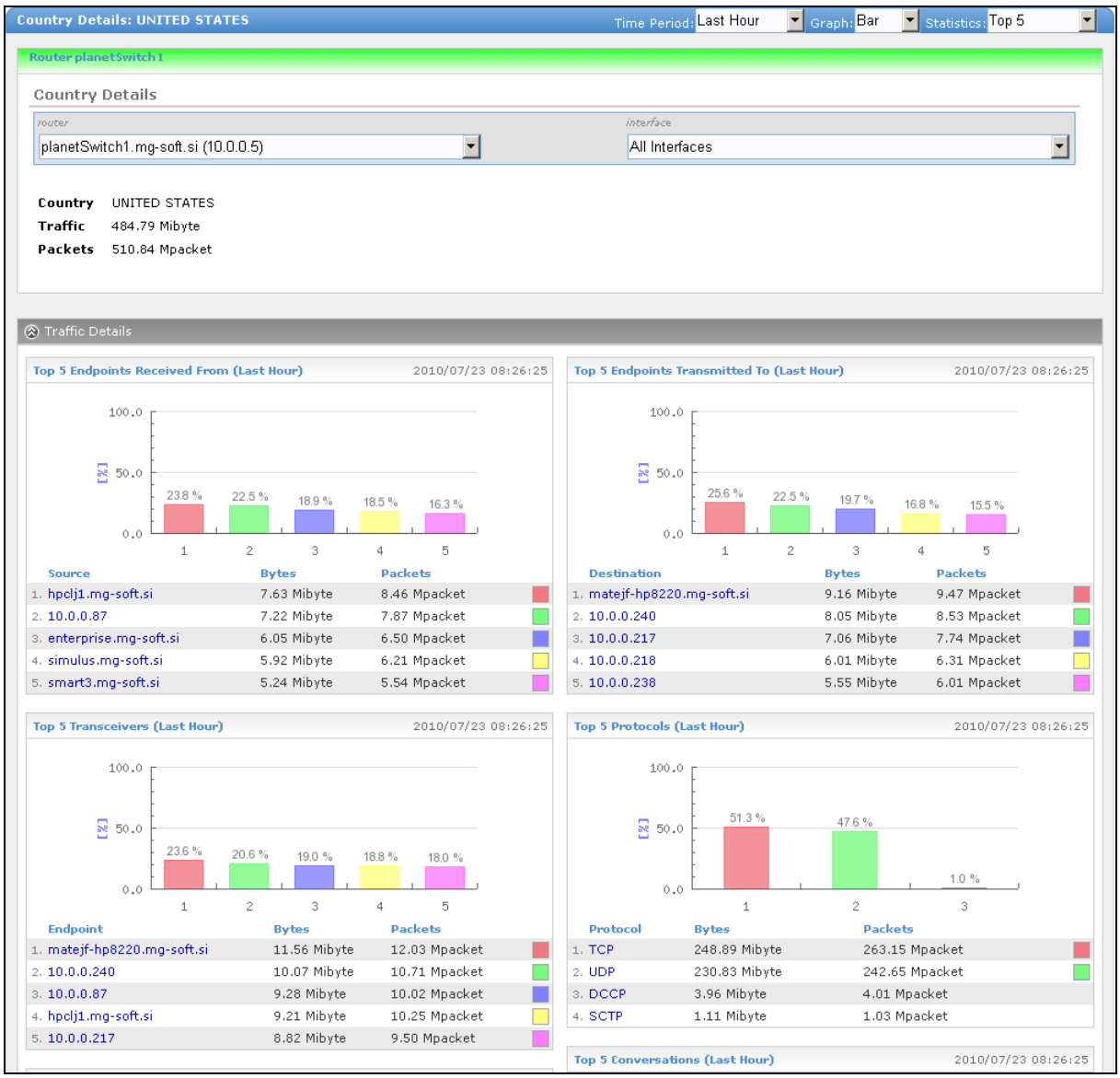

Country Details: UNITED STATES
Time Period: Last Hour
Graph: Bar
Statistics: Top 5
Router planetSwitch1
Country Details
router
planetSwitch1.mg-soft.si (10.0.0.5)
interface
All Interfaces
Country UNITED STATES
Traffic 484.79 Mibyte
Packets 510.84 Mpacket
Traffic Details
Top 5 Endpoints Received From (Last Hour) 2010/07/23 08:26:25
Source Bytes Packets
1. hpclj1.mg-soft.si 7.63 Mibyte 8.46 Mpacket
2. 10.0.0.87 7.22 Mibyte 7.87 Mpacket
3. enterprise.mg-soft.si 6.05 Mibyte 6.50 Mpacket
4. simulus.mg-soft.si 5.92 Mibyte 6.21 Mpacket
5. smart3.mg-soft.si 5.24 Mibyte 5.54 Mpacket
Top 5 Endpoints Transmitted To (Last Hour) 2010/07/23 08:26:25
Destination Bytes Packets
1. matejf-hp8220.mg-soft.si 9.16 Mibyte 9.47 Mpacket
2. 10.0.0.240 8.05 Mibyte 8.53 Mpacket
3. 10.0.0.217 7.06 Mibyte 7.74 Mpacket
4. 10.0.0.218 6.01 Mibyte 6.31 Mpacket
5. 10.0.0.238 5.55 Mibyte 6.01 Mpacket
Top 5 Transceivers (Last Hour) 2010/07/23 08:26:25
Endpoint Bytes Packets
1. matejf-hp8220.mg-soft.si 11.56 Mibyte 12.03 Mpacket
2. 10.0.0.240 10.07 Mibyte 10.71 Mpacket
3. 10.0.0.87 9.28 Mibyte 10.02 Mpacket
4. hpclj1.mg-soft.si 9.21 Mibyte 10.25 Mpacket
5. 10.0.0.217 8.82 Mibyte 9.50 Mpacket
Top 5 Protocols (Last Hour) 2010/07/23 08:26:25
Protocol Bytes Packets
1. TCP 248.89 Mibyte 263.15 Mpacket
2. UDP 230.83 Mibyte 242.65 Mpacket
3. DCCP 3.96 Mibyte 4.01 Mpacket
4. SCTP 1.11 Mibyte 1.03 Mpacket
Top 5 Conversations (Last Hour) 2010/07/23 08:26:25

Figure 35: Country Details page

3.4.8 Application Details Page

To open the ***Application Details page*** click an application name in the home page.

On this page you can monitor:

- Top N Servers,
- Top N Clients,
- Top N Server Receivers,
- Top N Server Transmitters,
- Top N Client Receivers,
- Top N Client Transmitters,
- Top N Client Countries,
- Top N Server Countries,
- Top N Conversations.

Note: in the upper right corner of the frame, you can select the **time period, graph** (bar or pie), **and the N** value for all **Top N** reports displayed in this page.

When you click on the name of an item, you are redirected to the appropriate page (Endpoint Details page if the item is an endpoint, Application Details page if the item is an application, etc.) displaying information related to that specific item on a specific router.

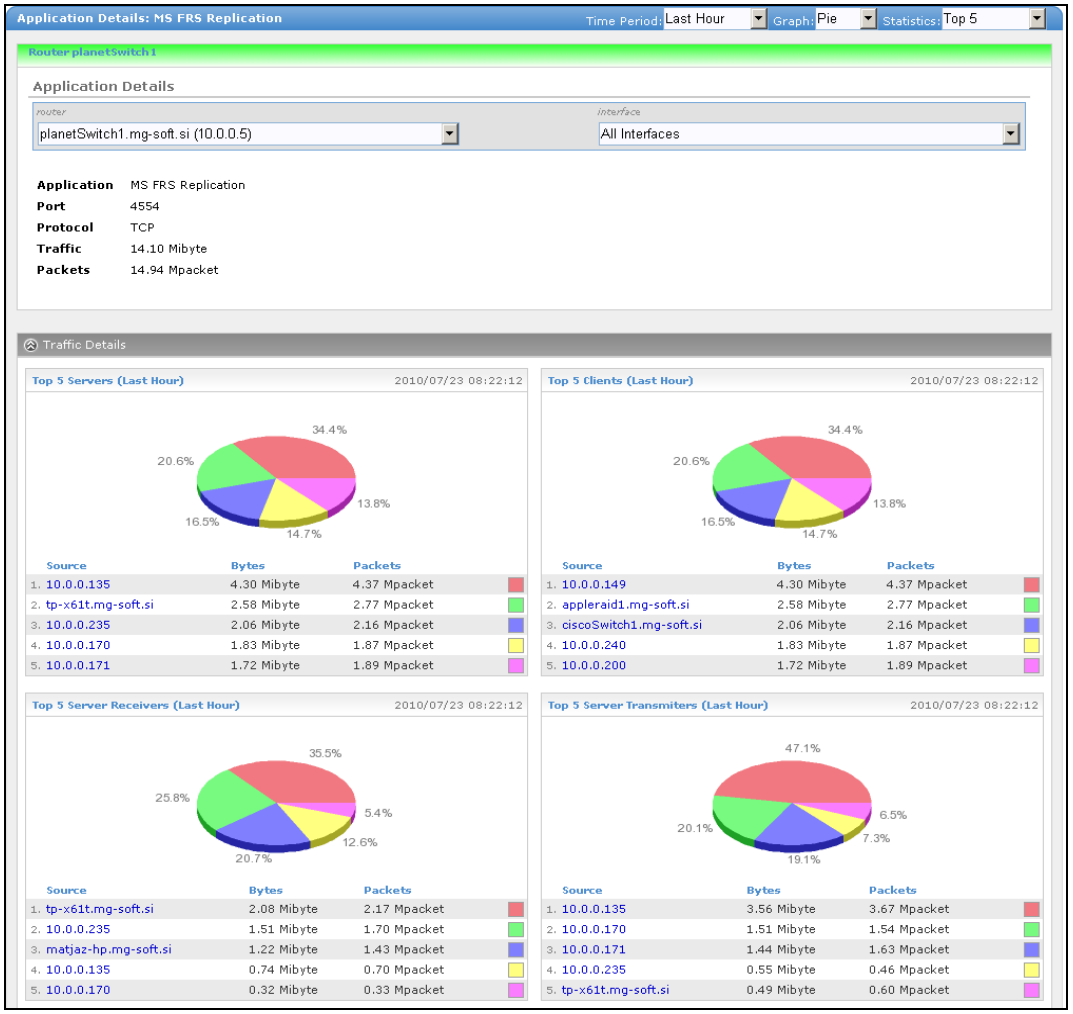


Figure 36: Application Details page

3.4.9 NetFlow Configuration Page

To configure the ***NetFlow*** home page click on the ***Configure*** button (nr.2 in Figure 26).

The Netflow Configuration Page appears (Figure 37).

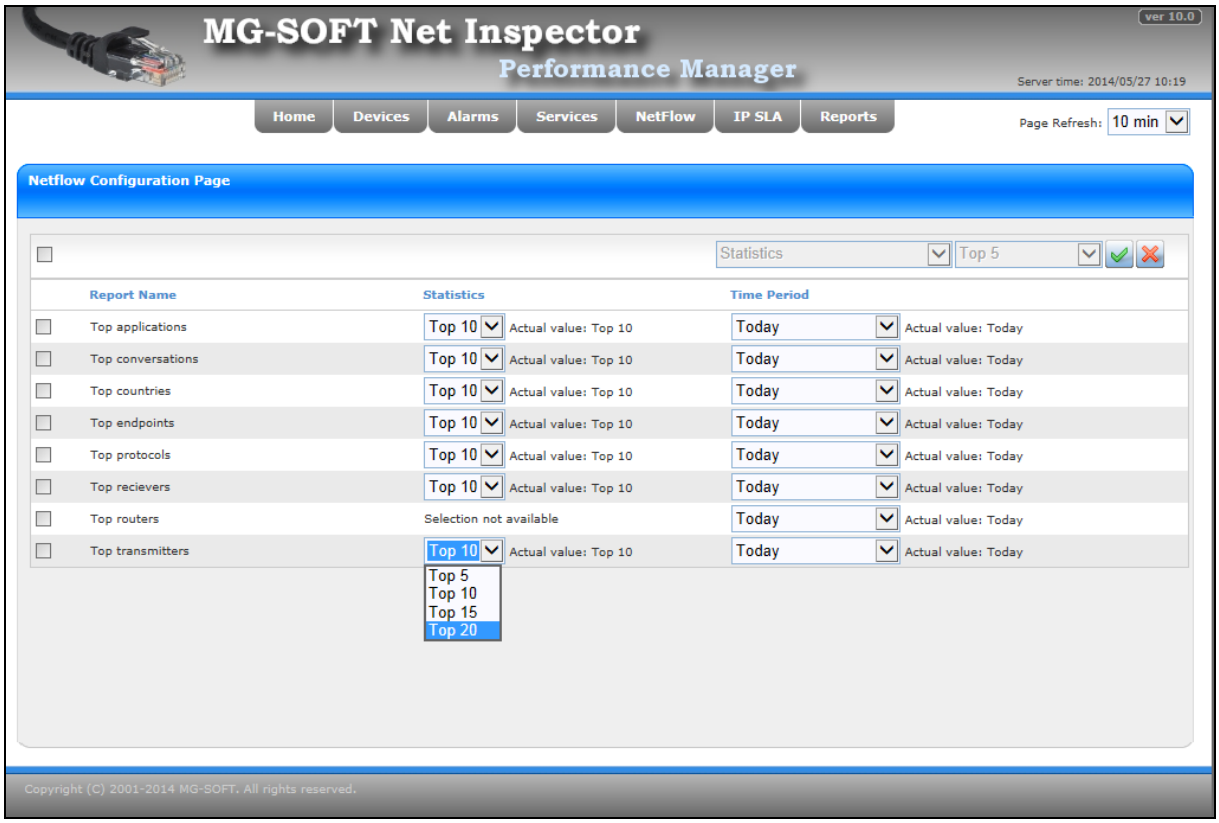


Figure 37: NetFlow Configuration Page

Here you can select how many entries (N) the individual Top N report will contain and for which time interval the data will be shown.

In the ***Statistics*** drop-down list, you can choose between the following Top N statistics:

- Top 5,
- Top 10,
- Top 15,
- Top 20.

In the ***Time Period*** drop-down list, you can choose among these the standard time periods.

To change the statistics and/or the time period, select the desired entry from the corresponding drop-down menu and click the ***Apply*** button ( ).

3.5 Monitoring Network Services

Net Inspector support monitoring of the following TCP and UDP network services: HTTP, HTTPS, FTP, DNS, SMTP, IMAP, IMAPS, POP3, SSH, Telnet, NNTP, NNTPS, SIP, H.323, LDAP, LDAPS, IPP, LPD, MsSQL, MySQL and Oracle service.

The monitoring of network services is enabled by default, meaning that managed objects (devices) are automatically scanned for the supported network services and detected services are automatically monitored by Net Inspector. You can customize which of the supported network services will be monitored on which device in the **Edit Device Monitoring Options** page – **Services tab**, as described in the Configuring Device Monitoring Options (Interfaces, Storage Units, Processes, Services) section.

Monitoring of network services can be disabled altogether in the polling profile that is assigned to the given device.

To open the Services page, click on the **Services** tab in the Performance Manager home page (Figure 38).

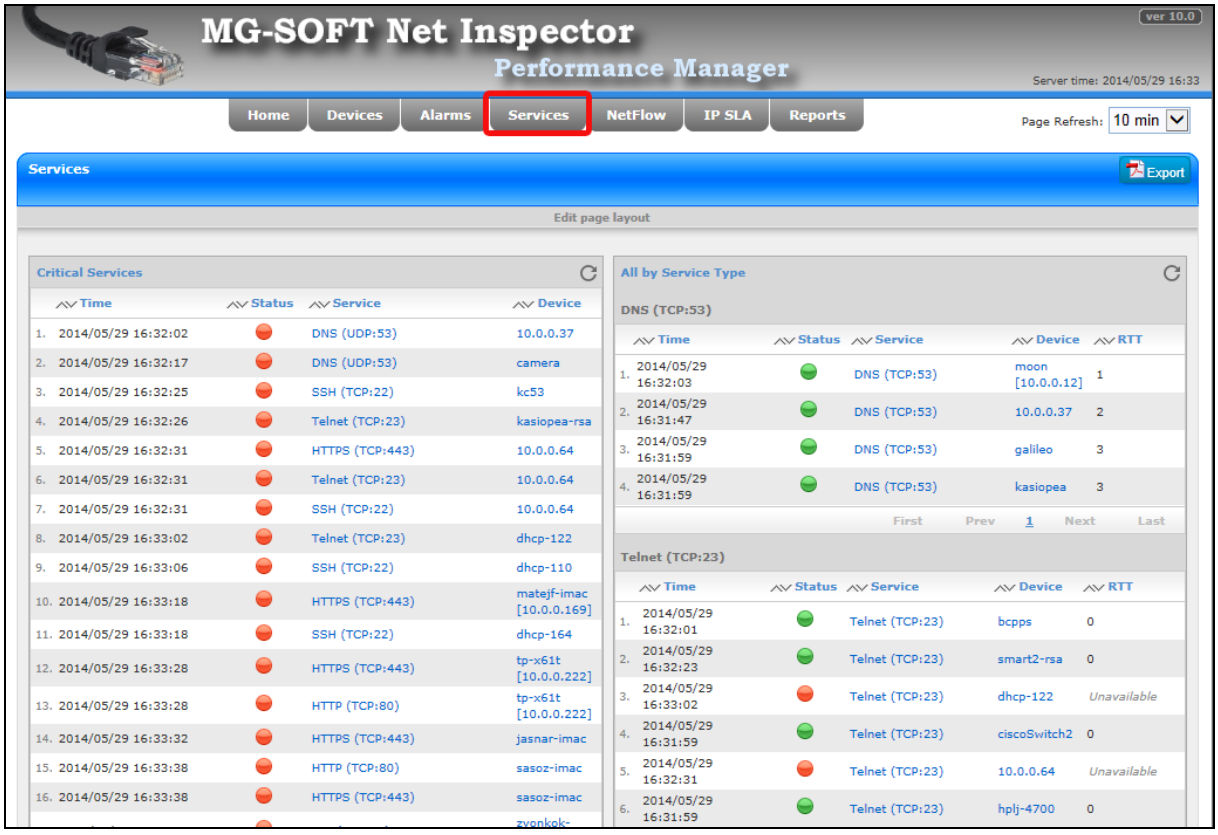

MG-SOFT Net Inspector
Performance Manager
ver 10.0
Server time: 2014/05/29 16:33
Home
Devices
Alarms
Services
NetFlow
IP SLA
Reports
Page Refresh: 10 min
Services
Export
Edit page layout
Critical Services
Time Status Service Device
1. 2014/05/29 16:32:02 DNS (UDP:53) 10.0.0.37
2. 2014/05/29 16:32:17 DNS (UDP:53) camera
3. 2014/05/29 16:32:25 SSH (TCP:22) kc53
4. 2014/05/29 16:32:26 Telnet (TCP:23) kasiopea-rsa
5. 2014/05/29 16:32:31 HTTPS (TCP:443) 10.0.0.64
6. 2014/05/29 16:32:31 Telnet (TCP:23) 10.0.0.64
7. 2014/05/29 16:32:31 SSH (TCP:22) 10.0.0.64
8. 2014/05/29 16:33:02 Telnet (TCP:23) dhcp-122
9. 2014/05/29 16:33:06 SSH (TCP:22) dhcp-110
10. 2014/05/29 16:33:18 HTTPS (TCP:443) matejf-imac [10.0.0.169]
11. 2014/05/29 16:33:18 SSH (TCP:22) dhcp-164
12. 2014/05/29 16:33:28 HTTPS (TCP:443) tp-x61t [10.0.0.222]
13. 2014/05/29 16:33:28 HTTP (TCP:80) tp-x61t [10.0.0.222]
14. 2014/05/29 16:33:32 HTTPS (TCP:443) jasnar-imac
15. 2014/05/29 16:33:38 HTTP (TCP:80) sasoz-imac
16. 2014/05/29 16:33:38 HTTPS (TCP:443) sasoz-imac
All by Service Type
DNS (TCP:53)
Time Status Service Device RTT
1. 2014/05/29 16:32:03 DNS (TCP:53) moon [10.0.0.12] 1
2. 2014/05/29 16:31:47 DNS (TCP:53) 10.0.0.37 2
3. 2014/05/29 16:31:59 DNS (TCP:53) galileo 3
4. 2014/05/29 16:31:59 DNS (TCP:53) kasiopea 3
First Prev 1 Next Last
Telnet (TCP:23)
Time Status Service Device RTT
1. 2014/05/29 16:32:01 Telnet (TCP:23) bcpps 0
2. 2014/05/29 16:32:23 Telnet (TCP:23) smart2-rsa 0
3. 2014/05/29 16:33:02 Telnet (TCP:23) dhcp-122 Unavailable
4. 2014/05/29 16:31:59 Telnet (TCP:23) ciscoSwitch2 0
5. 2014/05/29 16:32:31 Telnet (TCP:23) 10.0.0.64 Unavailable
6. 2014/05/29 16:31:59 Telnet (TCP:23) hplj-4700 0

Figure 38: Services page

The Services page displays a list all monitored services on devices by category (DNS, HTTP, IMAP, SSH,…) and a list of services with the status of “critical”. Critical status means that the service is currently not available.

Click a service in the list, to view more detailed statistics (service availability and round trip time (RTT) - current value and history) for the given service.

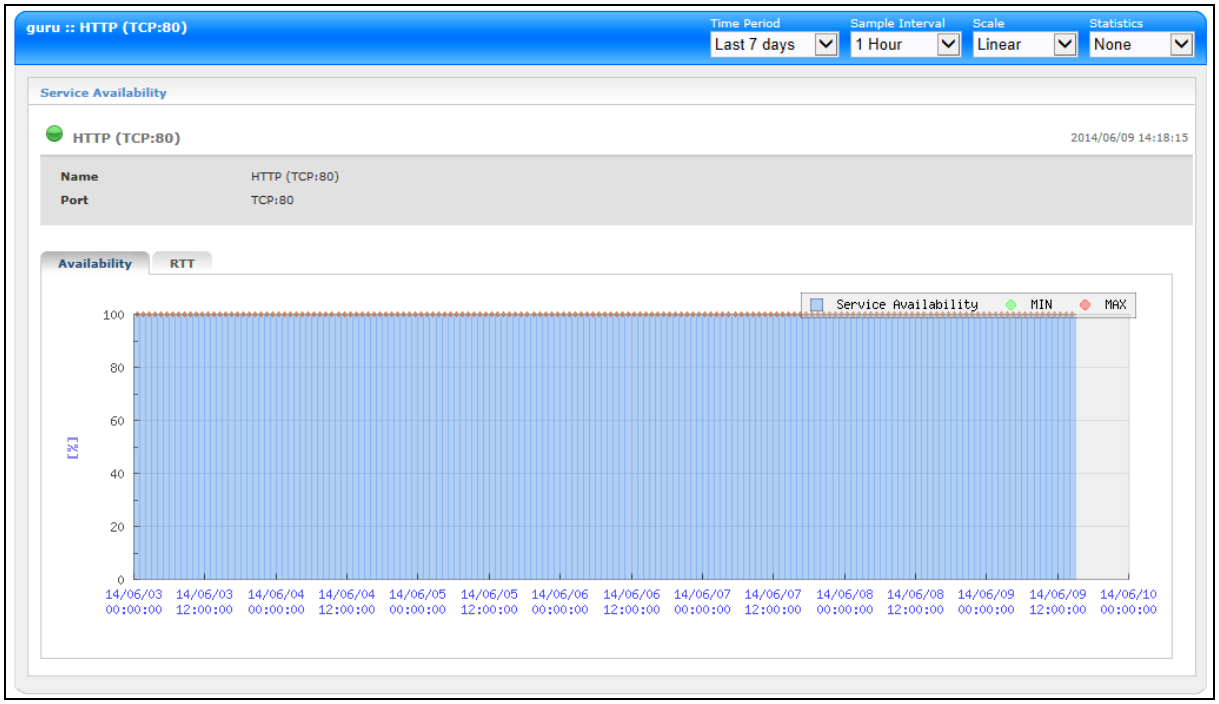


Figure 39: Viewing the availability history of a www service

Click the graph to view more detailed service availability information (graph and table showing the service availability statistics [in %]).

Click the **RTT** tab to view the latency [in ms] of the given service (Figure 40).

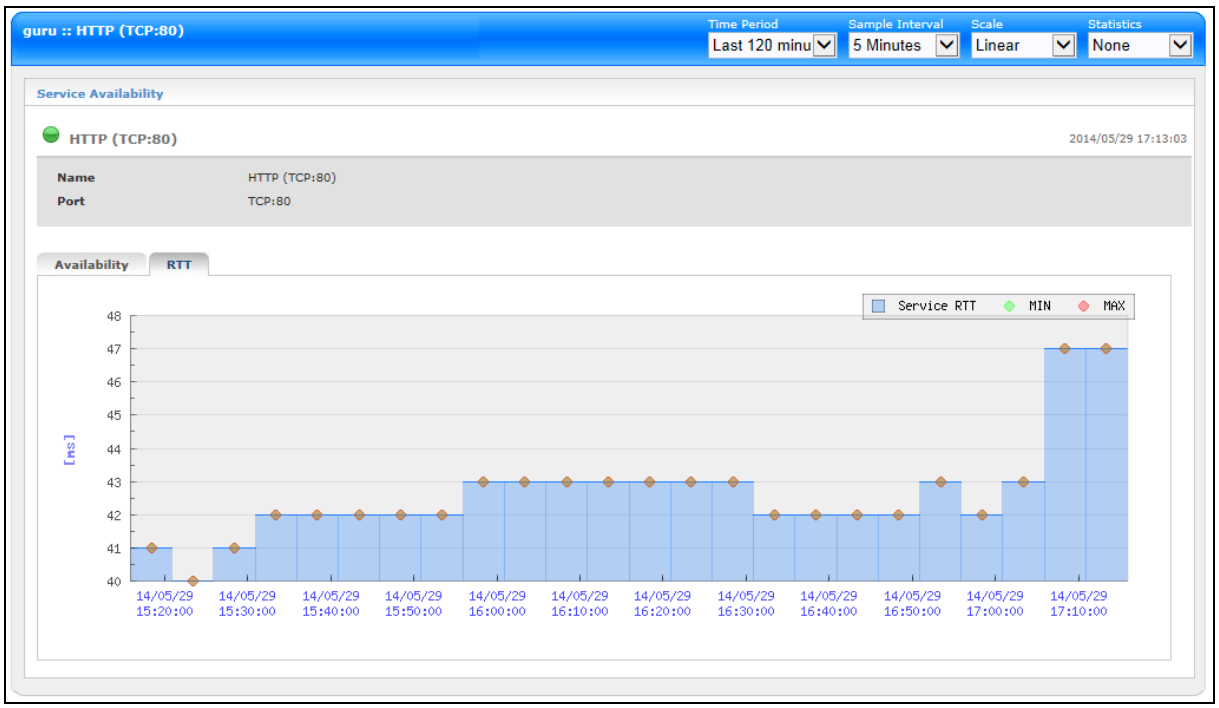


Figure 40: Viewing the latency history of a www service (HTTP Get request-response RTT)

3.6 IP SLA Monitoring

The IP SLA page contains the lists of IP SLA operations that are configured on your Cisco device. The operations (source ->destination items) are listed by different categories e.g., HTTP, DNS, Jitter (VoIP),... .

> For more information on configuring IP SLA operations on Cisco devices, please consult the Cisco documentation

To open the IP SLA page, click on the **IP SLA** tab in the Performance Manager home page.

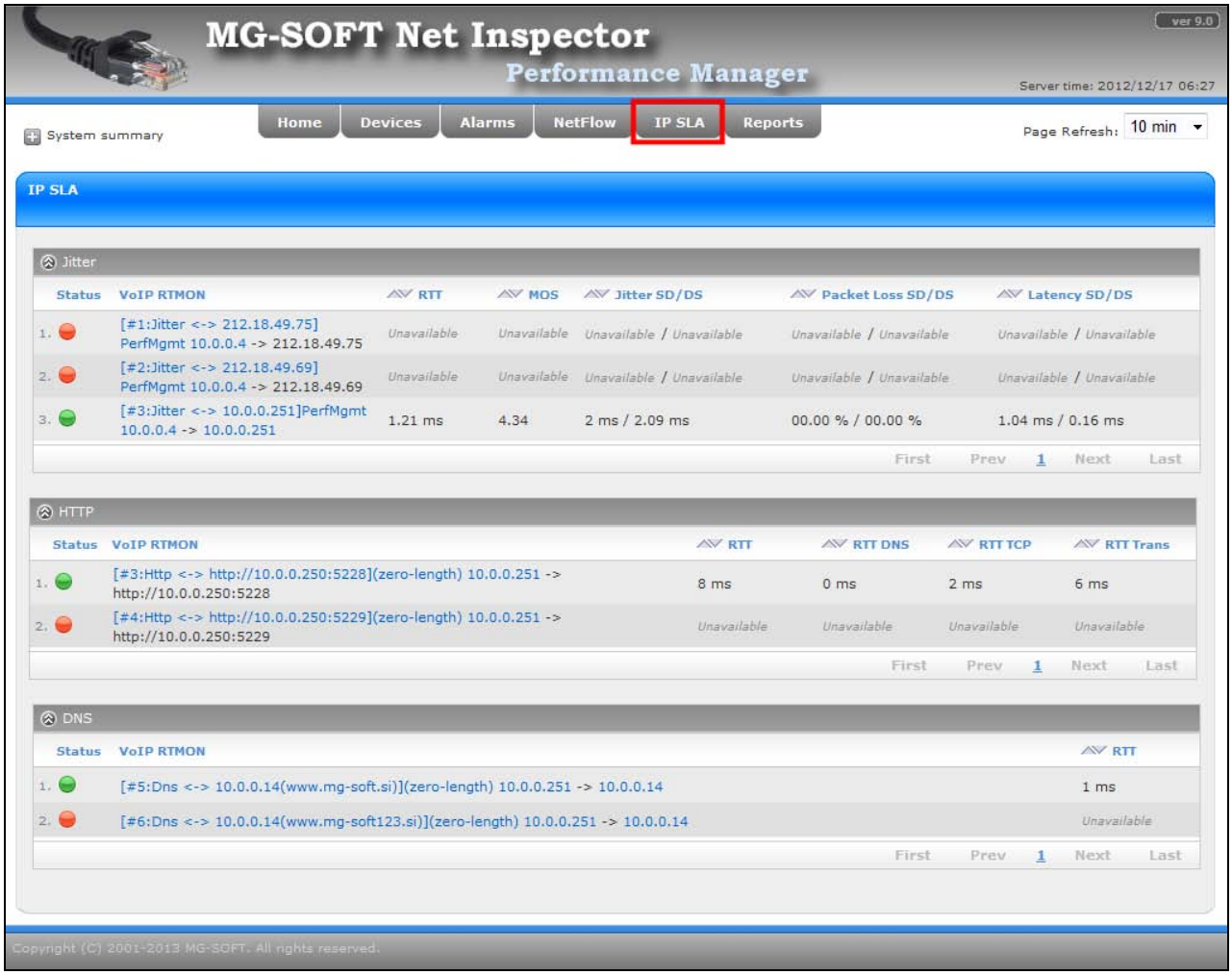

MG-SOFT Net Inspector
Performance Manager
ver 9.0
Server time: 2012/12/17 06:27
System summary
Home
Devices
Alarms
NetFlow
IP SLA
Reports
Page Refresh: 10 min
IP SLA
Jitter
Status VoIP RTMON RTT MOS Jitter SD/DS Packet Loss SD/DS Latency SD/DS
1. [#1:Jitter <-> 212.18.49.75] PerfMgmt 10.0.0.4 -> 212.18.49.75 Unavailable Unavailable Unavailable / Unavailable Unavailable / Unavailable Unavailable / Unavailable
2. [#2:Jitter <-> 212.18.49.69] PerfMgmt 10.0.0.4 -> 212.18.49.69 Unavailable Unavailable Unavailable / Unavailable Unavailable / Unavailable Unavailable / Unavailable
3. [#3:Jitter <-> 10.0.0.251]PerfMgmt 10.0.0.4 -> 10.0.0.251 1.21 ms 4.34 2 ms / 2.09 ms 00.00 % / 00.00 % 1.04 ms / 0.16 ms
First Prev 1 Next Last
HTTP
Status VoIP RTMON RTT RTT DNS RTT TCP RTT Trans
1. [#3:Http <-> http://10.0.0.250:5228](zero-length) 10.0.0.251 -> http://10.0.0.250:5228 8 ms 0 ms 2 ms 6 ms
2. [#4:Http <-> http://10.0.0.250:5229](zero-length) 10.0.0.251 -> http://10.0.0.250:5229 Unavailable Unavailable Unavailable Unavailable
First Prev 1 Next Last
DNS
Status VoIP RTMON RTT
1. [#5:Dns <-> 10.0.0.14(www.mg-soft.si)](zero-length) 10.0.0.251 -> 10.0.0.14 1 ms
2. [#6:Dns <-> 10.0.0.14(www.mg-soft123.si)](zero-length) 10.0.0.251 -> 10.0.0.14 Unavailable
First Prev 1 Next Last
Copyright (C) 2001-2013 MG-SOFT. All rights reserved.

Figure 41: IP SLA page

By clicking an item in the first column (e.g., VoIP RTTMON), you can view more detailed statistics with history for the given IP SLA operation. For VoIP, this includes the mean opinion score (MOS), round trip time (RTT), jitter, packet loss, latency, packet out of sequences, packet MIA, packet late arrivals and other IP SLA statistics.

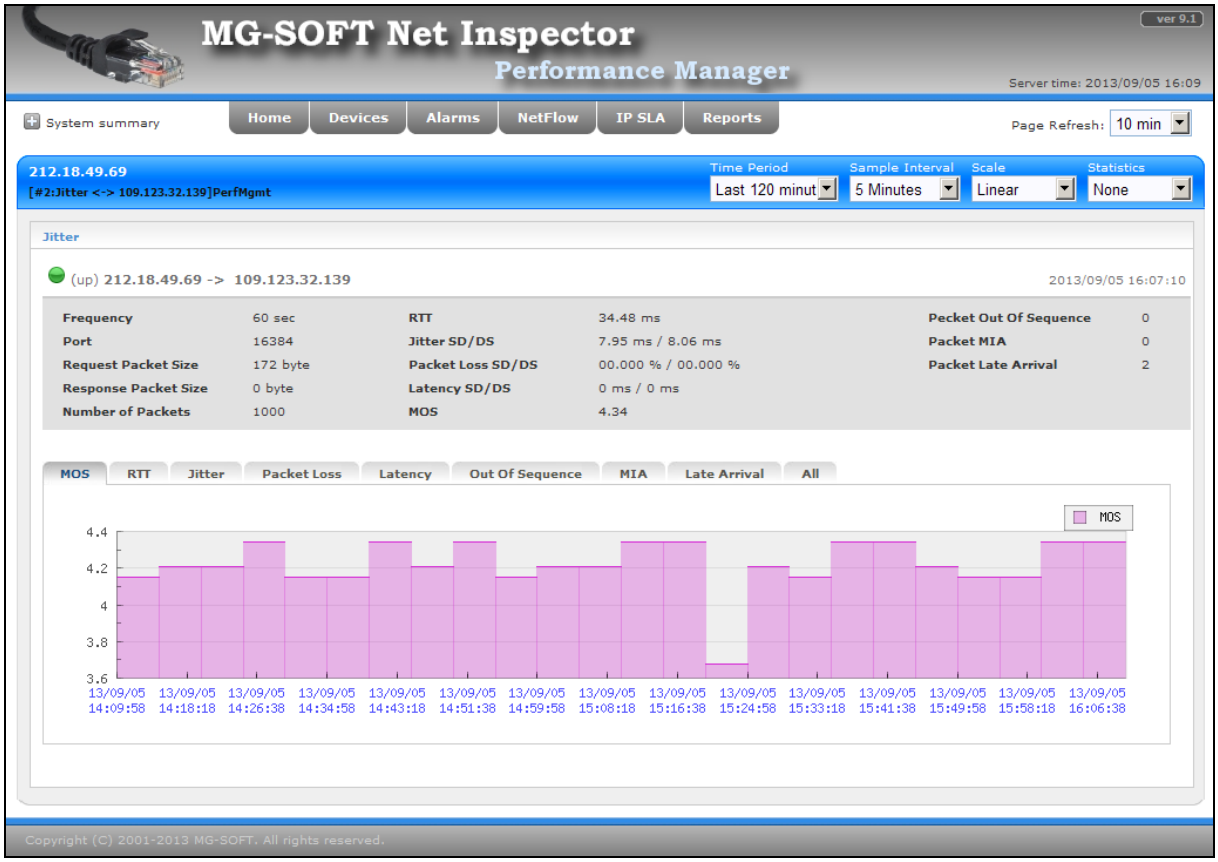


Figure 42: Example of a web page displaying the IP SLA VoIP quality statistics (MOS)

Click any tab (Jitter, Packet Loss, Latency, MOS, etc.) or graph to view more data for the given metric.

4 VIEWING AND CREATING REPORTS

Net Inspector Performance Manager offers a set of predefined fault and performance management reports (e.g., device availability, number of alarms per severity, network interface utilization,…) and lets you configure your own reports based on the built-in statistics or user-defined custom polling statistics.

4.1 Viewing Predefined Reports

Net Inspector Performance Manager comes with a series of predefined fault and performance management reports (e.g., device availability, number of alarms per severity, network interface utilization,…) that are accessible out-of-the-box. A user can select the desired time interval (e.g., day, week, month, quarter, year,…) for any of the predefined time reports and results are displayed in a tabular form either for all managed devices in the currently active user view or only for a subset of devices specified by a filter. Results can be sorted by any column included in reports (e.g., device name, availability, number of alarms, discarded packets, min. and max. values, etc.). All predefined reports, except NetFlow reports, contain the average values for the selected time interval, and where applicable, also minimum and maximum values within this interval (e.g., Response Time report for one day contains the average response times for devices in the given day, as well as the absolute min. and max. device response times within that day). Predefined reports (also termed time reports) can be exported to PDF and CSV file formats for external viewing or post-processing.

This section describes how to select and view the predefined time reports.

1. Click the ***Reports*** tab in the main window to display the **Reports** page (Figure 43).
2. The **Time reports** frame (Figure 43) in the **Reports** page displays a list of predefined reports in different categories (e.g., Interfaces, Host resources, Services, etc.). Click a category to view all time reports that belong to it. Then, click the individual report within the category to open it. The categories are:
   - Status: device availability (reachability), response time and packet loss reports
   - Fault: fault management reports (number of alarms per severity, alarm duration and frequency, etc.)
   - Interfaces: network interface-related reports (input/output utilization, traffic, error rate, etc.)
   - Host resources: system resources usage reports (CPU, memory, storage volumes)
   - Processes: monitored processes reports (process running status, CPU usage, memory usage)
   - Services: service availability, service round trip time (RTT)
   - Cisco: Cisco-specific resources usage reports (memory, interfaces) and Cisco IP SLA-specific reports (round trip times for ICMP, HTTP, DNS, VoIP jitter, VoIP MOS, etc.)

- NetFlow: NetFlow reports (TopN applications, transceivers, protocols, conversations or countries for the selected router (or all routers) and interface (or all interfaces))

Optionally, use the ***Search*** facility in the right portion of the **Time Reports** frame to quickly find the reports that matches the entered search phrase. Click the report you want to view in the **Time Reports** frame.

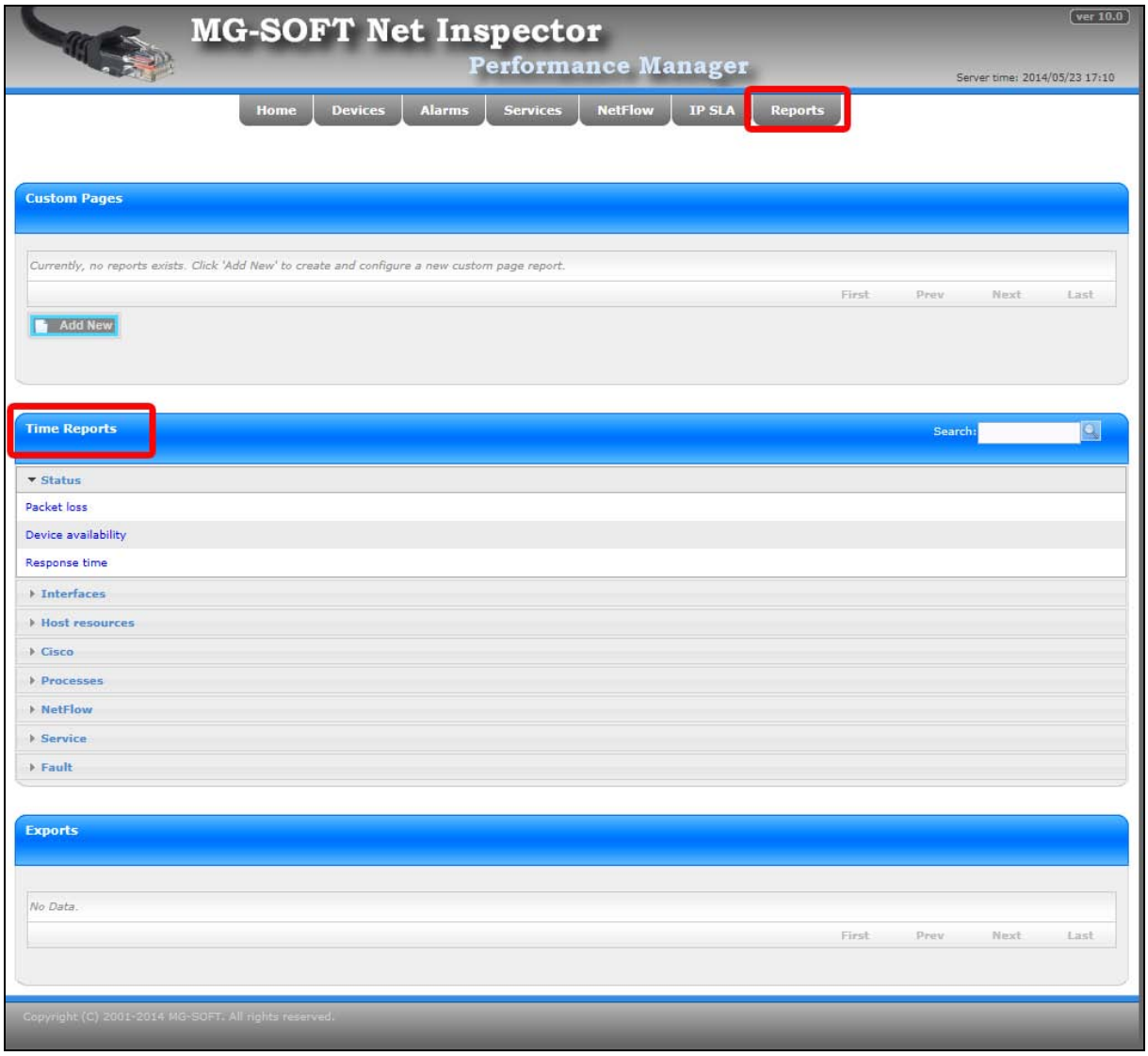


Figure 43: Selecting a predefined time report from the Reports page

3. The selected report is displayed for the current day (Figure 44). You can sort the report items by any column (e.g., device name, value, min., max. value) by clicking the sort symbol ( ) in the header of the respective column.
4. To view the report for a different time frame, select the desired category from the **Time interval** toolbar drop-down list (e.g., day, week, month, quarter, year etc.) and optionally shift the displayed time frame forward or backward by clicking the arrow buttons ( ) in the **Time interval** toolbar. When the desired time interval for the report is selected, click the ***Apply*** button in the right section of the **Time interval** toolbar to update the report to include the data for the new time interval.

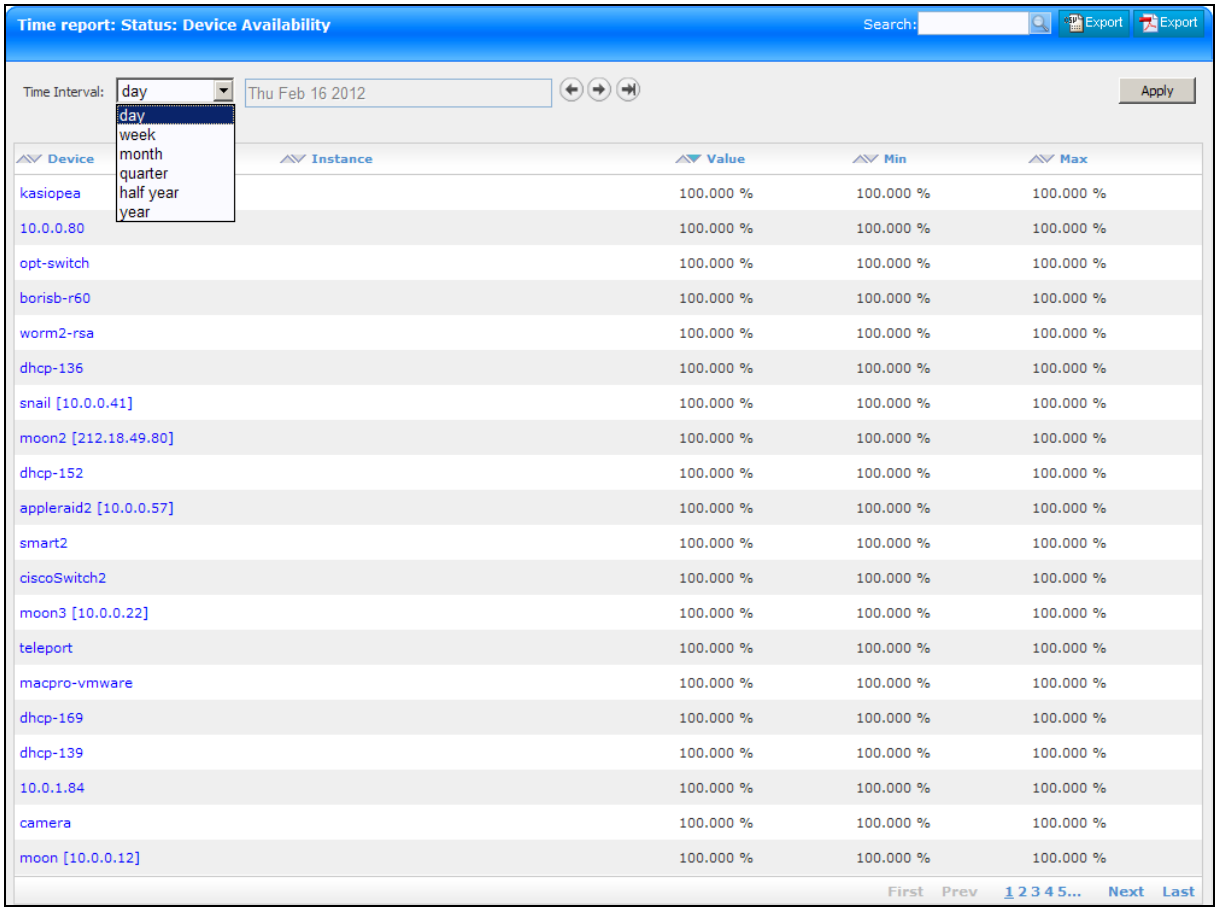


Figure 44: Viewing a predefined time report (Device Availability)

5. To export the displayed report to PDF or CSV (comma-separated values) file format, click the respective button (

) in the report titlebar frame. A dialog that papers prompts you to save the report to a file or open it. Select the desired option and click the ***OK*** button. After a report has been exported, it is also automatically added to the **PDF Exports** frame in the **Reports** page.

4.2 Creating Custom Reports

Net Inspector Performance Manager lets you configure custom report pages, containing graphs or tables displaying metrics monitored on one or more devices. Examples of such custom reports are Top5 reports, reports of monitored objects with problems, etc.

You can also create “device map” reports containing a bitmap image (e.g., a map, office floor plan…) and then position icons that represent managed devices on that map.

In addition, web report pages can be converted to PDF format.

This section describes how to configure:

- A typical custom report page (HTML).
- A device map report page and how to place managed object on it to enable monitoring device statuses and alarms on the map.

4.2.1 Creating Custom Report Pages

This section describes how to configure a typical custom report page showing Top5 devices by CPU load.

Custom report pages can contain more than one object (graph or table), as described in the next section.

1. Click the ***Reports*** tab in the main window to display the **Reports** page (Figure 45).

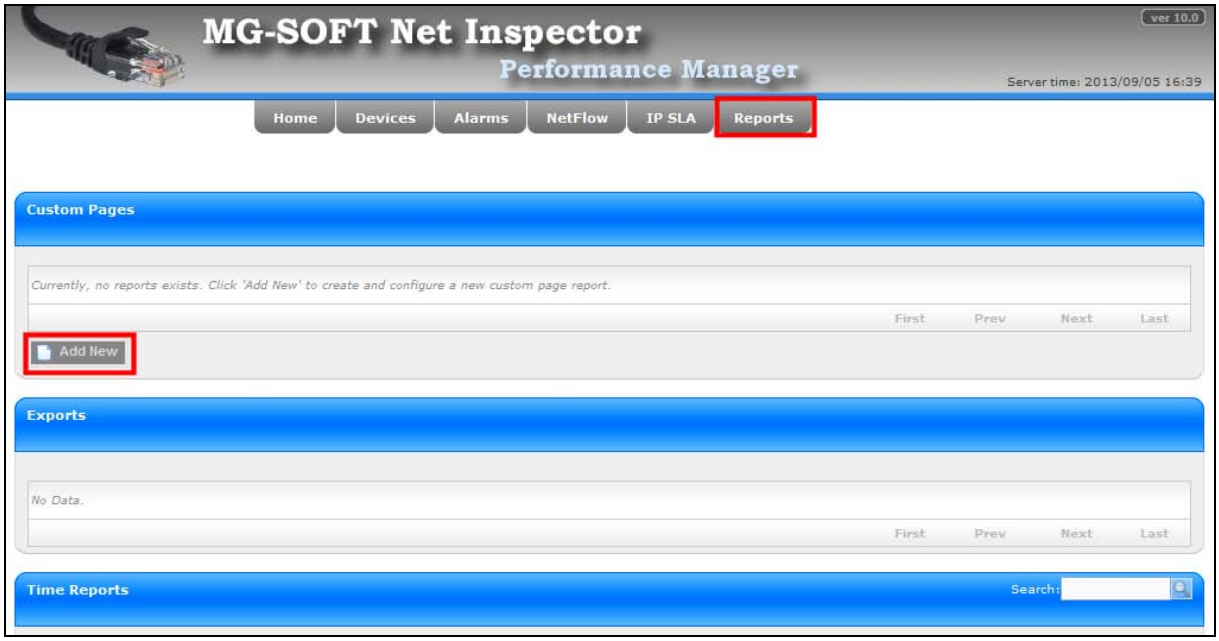


Figure 45: Reports page

2. In the ***Custom pages*** frame, click the ***Add New*** button (Figure 45) to start configuring a custom report page.
3. The ***Custom Report Page*** configurator appears (Figure 47).
4. Into the ***Custom page title*** input line, enter the title of the custom report page you are creating.
5. A custom report page can contain 1, 2 or 3 columns. Select the desired number of columns from the ***Number of columns*** drop-down list in the **Edit Page Layout** drop-down frame (Figure 46).

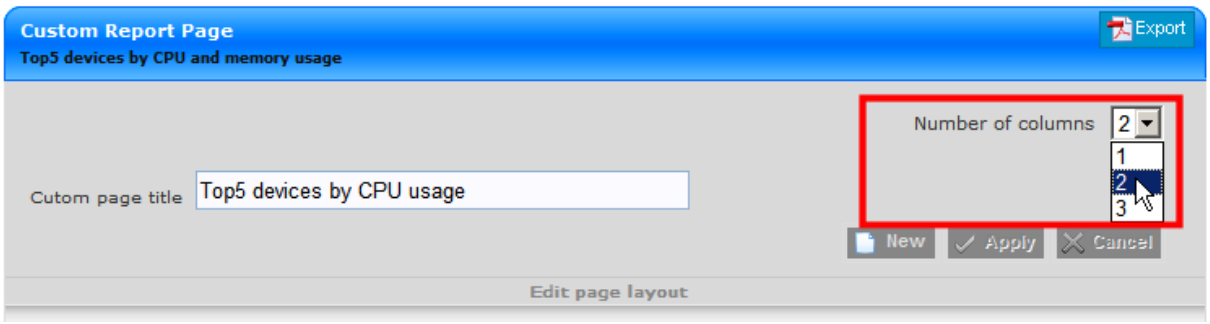


Figure 46: Setting the number of columns for a custom report page

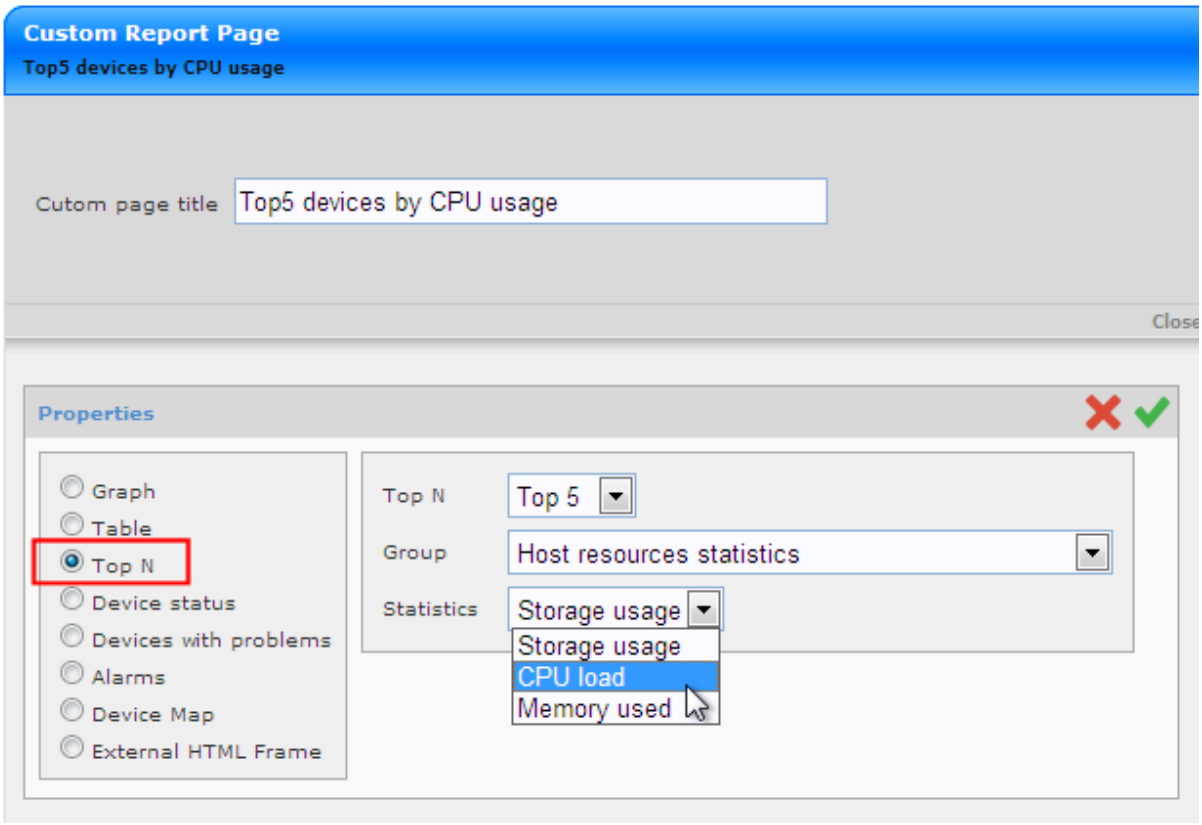


Figure 47: Example of setting a Top5 report properties in the custom page configurator

6. In the ***Properties*** frame, you can select one of the following report types:
   - ***Graph*** – lets you create a report page containing any of the graphs available in Net Inspector Performance Manager for one or more devices (here, a graph of all numeric parameters collected through SNMP and ICMP ping can be selected, like the device response time, packet loss, availability, interface-related statistics, host resources-related statistics, Cisco-related statistics (including IP SLA), processes and services statistics, etc.). For these reports, the desired time interval, granularity (sample interval), graph scale and value category (raw, min., max) can be selected as well as additional properties for some of the statistics.
   - ***Table*** – lets you create a report page containing any of the tables available in Net Inspector Performance Manager (here, all parameters collected through SNMP and ICMP ping can be selected, like the device response time, packet loss, availability, interface-related statistics, host resources-related statistics, Cisco-related statistics (including IP SLA), processes and services statistics, etc.). For these reports, the desired time interval, granularity (sample interval), samples per page and value category (raw, min., max) can be selected as well as additional properties for some of the statistics.
   - ***Top N*** – lets you select a report that displays only those N devices (N=5,10,20 etc.), whose latest values are the highest for the given metric (e.g., response time, packet loss, CPU usage, memory usage, interface, utilization etc.).
   - ***Device status*** – lets you select a report that displays a list of devices and their current statuses. A list can include either all devices or a subset of devices in the system.

- ***Devices with problems*** – lets you select a report that displays a list of devices with one or more open alarms. A minimum severity level of alarms included on the list can be selected.
- ***Alarms*** - lets you select a report that displays a list of active alarms. A list can be made either for all devices or a subset of devices in the system.
- ***Device map*** – lets you create a "device map" report page containing a bitmap image (e.g., a map, office floor plan…) as the background and managed object icons placed on the map.
- ***External HTTP frame*** – les you create a report page containing an existing HTTP page on any web site, select the ***External HTTP frame*** item and enter its URL and size in pixels in the accompanying input lines.

7. Depending on the type pf the custom report page you have selected in the left portion of the ***Properties*** frame, a different set of options is available in the frame of the right hand-side. Select the desired options from the drop-down list on the right hand-side (in our example, we selected the ***Top 5***, ***Host resources statistics*** and ***CPU load*** options).
8. Click the ***OK*** button (✔) in the ***Properties*** frame to create and view the new report page containing one object (=table of 5 devices with currently highest CPU usage). Note that custom report pages are dynamic in nature, meaning that their content is automatically updated (when the page is refreshed) to reflect the current state (i.e., to always display those 5 devices that have the highest CPU load at that time).

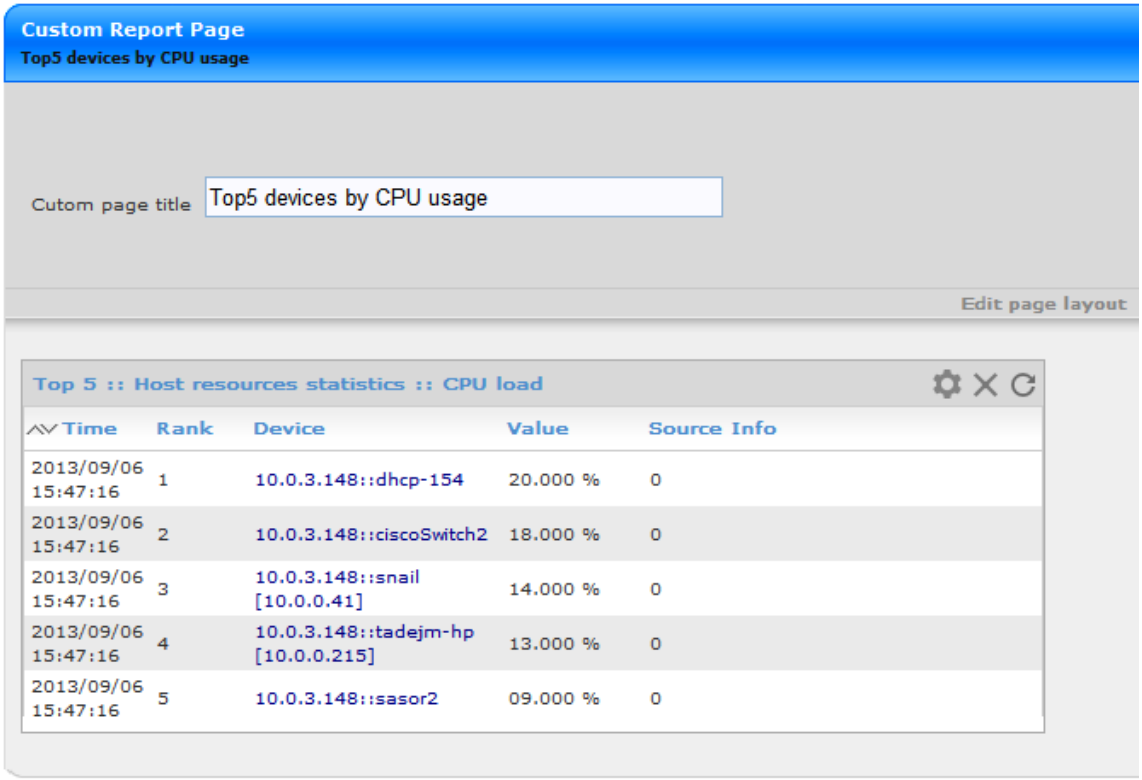


Figure 48: Viewing custom report page containing one object (table)

9. The custom report page is now created and available for viewing to all users with the same privileges (Figure 49).

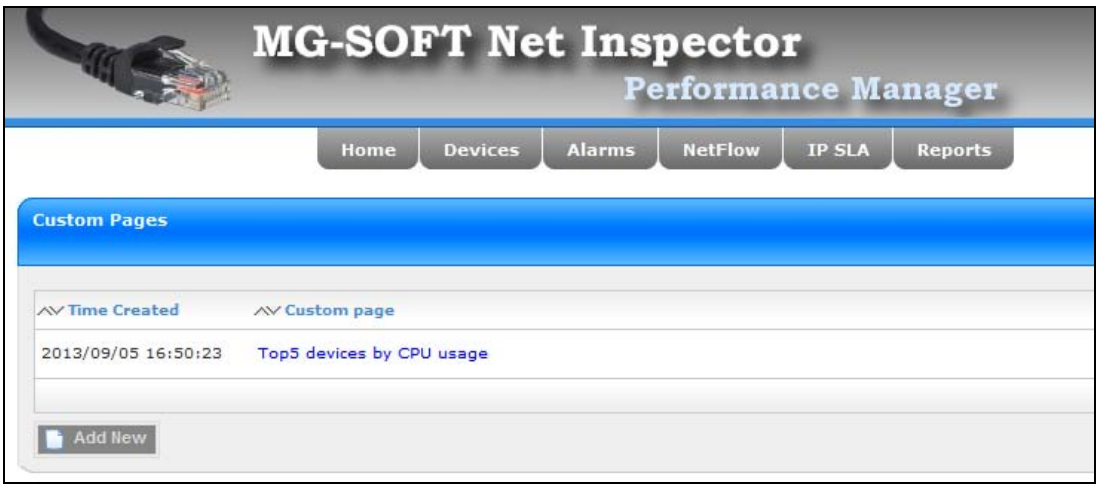


Figure 49: Reports page with one custom report page

4.3 Editing Custom Report Pages

Custom report pages can be edited, for example, to include additional objects (tables, graphs) or to include more instances of a monitored variable in an existing graph.

1. Click the ***Reports*** tab in the main window to display the **Reports** page (Figure 49).
2. In the **Custom report pages** frame, click the existing custom report page item that you would like to edit (Figure 50).

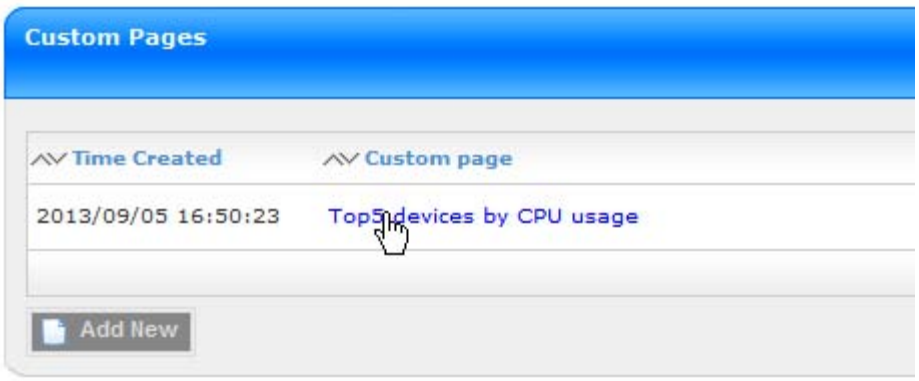


Figure 50: Opening a custom report page

3. The custom report page is displayed (Figure 51). Every custom report page contains one ore more rows, and every row contains zero or more objects: tables or graphs (depending on the value set in the ***Number of columns*** drop-down list) The custom page displayed below contains one row and one object within this row (Top5 devices by CPU usage table).

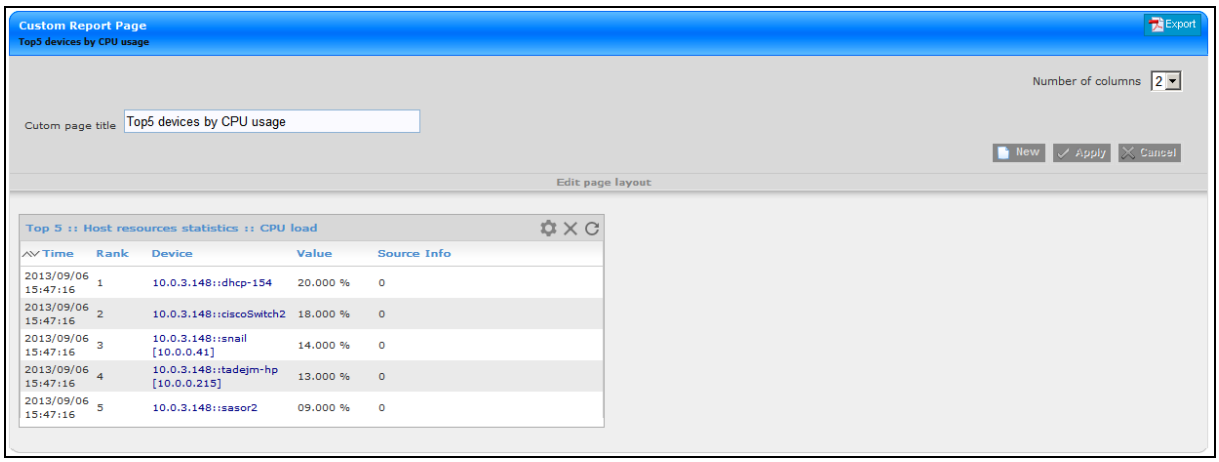

Custom Report Page
Top5 devices by CPU usage
Export
Number of columns 2
Cutom page title Top5 devices by CPU usage
New
Apply
Cancel
Edit page layout
Top 5 :: Host resources statistics :: CPU load
Time Rank Device Value Source Info
2013/09/06 15:47:16 1 10.0.3.148::dhcp-154 20.000 % 0
2013/09/06 15:47:16 2 10.0.3.148::ciscoSwitch2 18.000 % 0
2013/09/06 15:47:16 3 10.0.3.148::snail [10.0.0.41] 14.000 % 0
2013/09/06 15:47:16 4 10.0.3.148::tadejm-hp [10.0.0.215] 13.000 % 0
2013/09/06 15:47:16 5 10.0.3.148::sasor2 09.000 % 0

Figure 51: Viewing a custom report page in page configurator

To Add New Object (Table or Graph) to Page

1. To add an additional object (table or graph) to the row above (Figure 51), make sure to select number **2** in the ***Number of columns*** drop-down list in the ***Edit page layout frame***.

2. Then, click the ***New*** button (New) in the ***Edit page layout frame*** to add a new object next to the existing one in the custom page configurator (Figure 52).

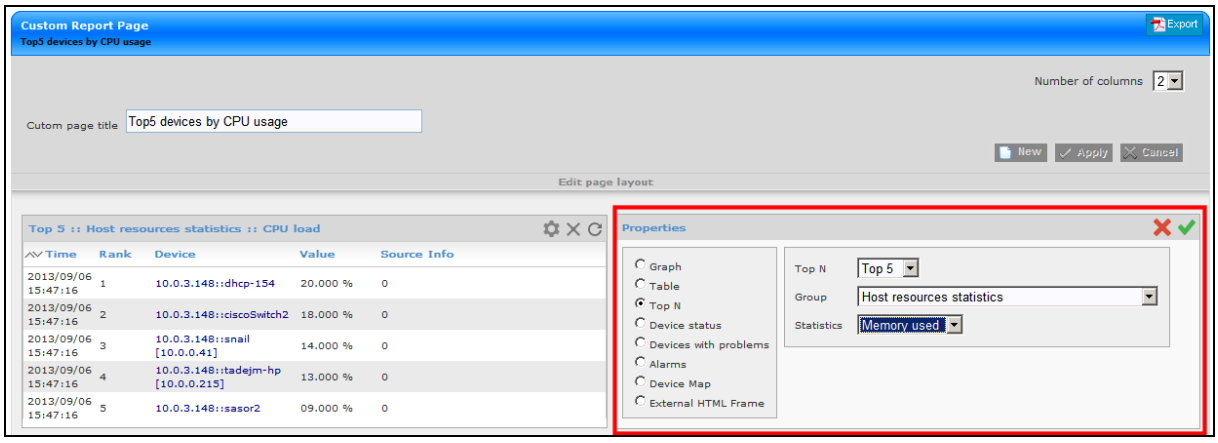


Figure 52: Configuring a second object in the custom report page

3. Select the appropriate entries in the ***Properties*** frame in the page configurator (Figure 52) by following the steps 1-6 described in the Creating Custom Report Pages section.

4. When you have finished configuring the settings for the new object, click the ***OK*** button ( ) in the ***Properties*** frame to create and view the report page containing both objects (Figure 53).

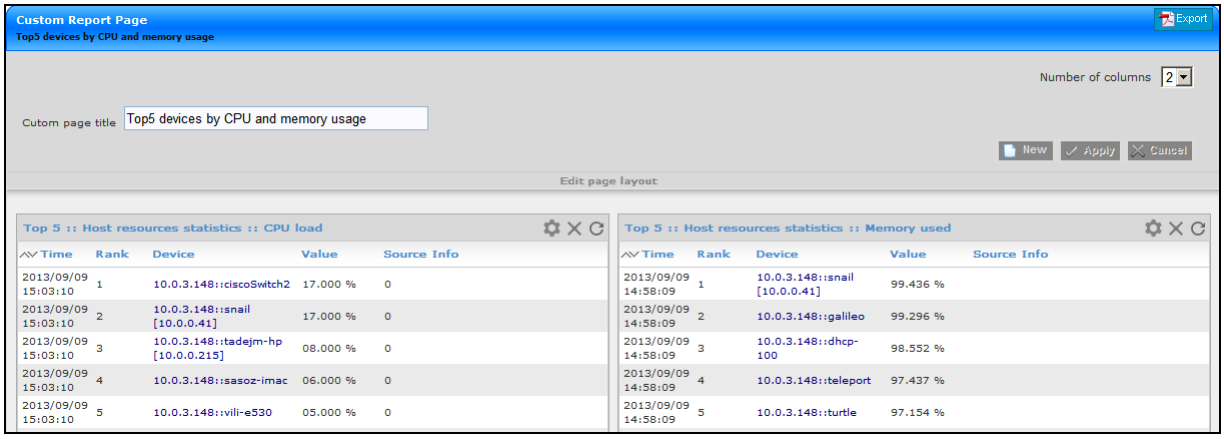

Custom Report Page
Top5 devices by CPU and memory usage
Export
Number of columns 2
Cutom page title Top5 devices by CPU and memory usage
New
Apply
Cancel
Edit page layout
Top 5 :: Host resources statistics :: CPU load
Time Rank Device Value Source Info
2013/09/09 15:03:10 1 10.0.3.148::ciscoSwitch2 17.000 % 0
2013/09/09 15:03:10 2 10.0.3.148::snail [10.0.0.41] 17.000 % 0
2013/09/09 15:03:10 3 10.0.3.148::tadejm-hp [10.0.0.215] 08.000 % 0
2013/09/09 15:03:10 4 10.0.3.148::sasoz-imac 06.000 % 0
2013/09/09 15:03:10 5 10.0.3.148::vili-e530 05.000 % 0
Top 5 :: Host resources statistics :: Memory used
Time Rank Device Value Source Info
2013/09/09 14:58:09 1 10.0.3.148::snail [10.0.0.41] 99.436 %
2013/09/09 14:58:09 2 10.0.3.148::galileo 99.296 %
2013/09/09 14:58:09 3 10.0.3.148::dhcp-100 98.552 %
2013/09/09 14:58:09 4 10.0.3.148::teleport 97.437 %
2013/09/09 14:58:09 5 10.0.3.148::turtle 97.154 %

Figure 53: Custom report page with two objects (tables) in a row

5. To move a frame to a different location in the custom report page, click the titlebar of the frame, hold down the left mouse button and drag the frame to the desired position. The shaded down-arrow markers appear at the location where the dropped frame will be positioned (Figure 16). Release the left mouse button to drop the frame to the marked position.
6. After repositioning the frames, click the ***Apply*** button (Apply) in the ***Edit page layout frame*** to permanently apply the changes.
7. Click the ***Edit page layout*** sign to close the drop-down frame.

To Add New Line to Graph

Many graphs and tables can contain more than one instance of a monitored parameter (variable). This section describes how to add an additional instance of interface inbound traffic to the existing graph, so that the values from two different interfaces (and devices) can be compared on the same graph.

1. Open the report page containing a graph in the page configurator as described in section Editing Custom Report Pages.
2. In the titlebar of the graph which you want to add an additional variable to, click the ***Edit*** button ( ). The graph Properties frame appears displaying the graph settings (Figure 54).
3. In the graph Properties frame, click the ***Add Variable*** button (Figure 54).

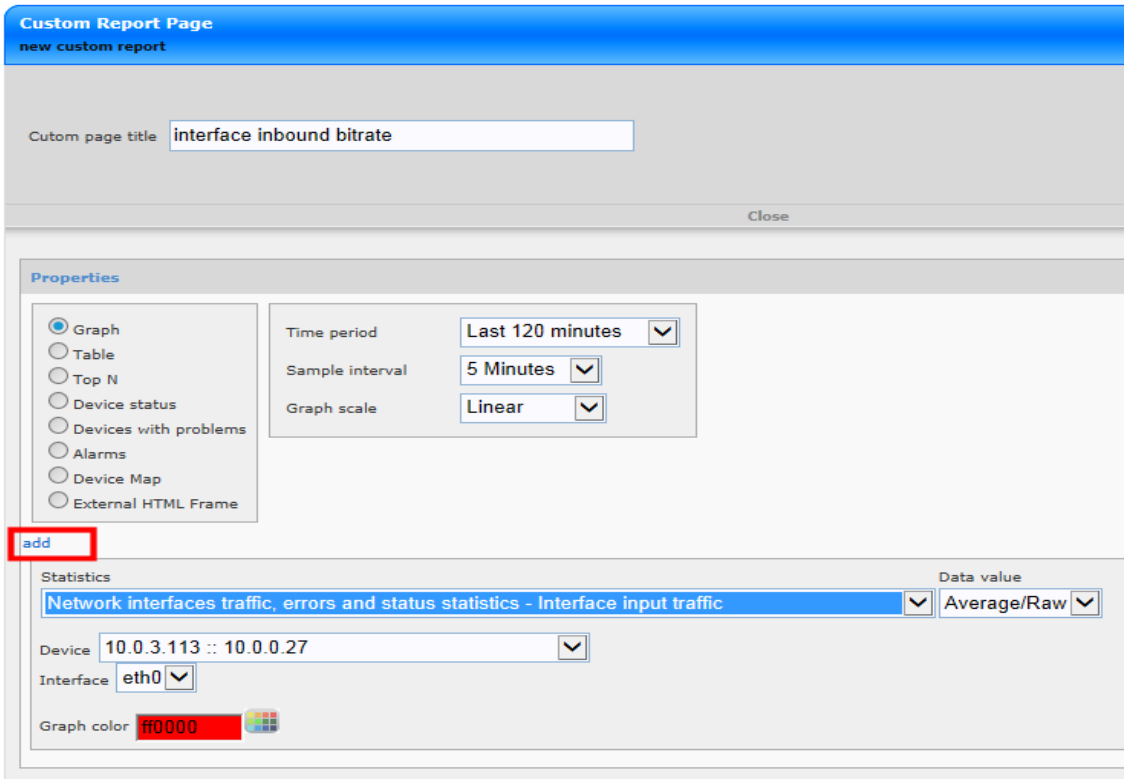


Figure 54: Clicking the Add Variable button in an existing graph

4. Another variable frame (Statistics, Device, Interface…) appears below the existing one. In the second frame select the device and interface you want to monitor as the second variable on the same graph and choose the variable color (Figure 55).

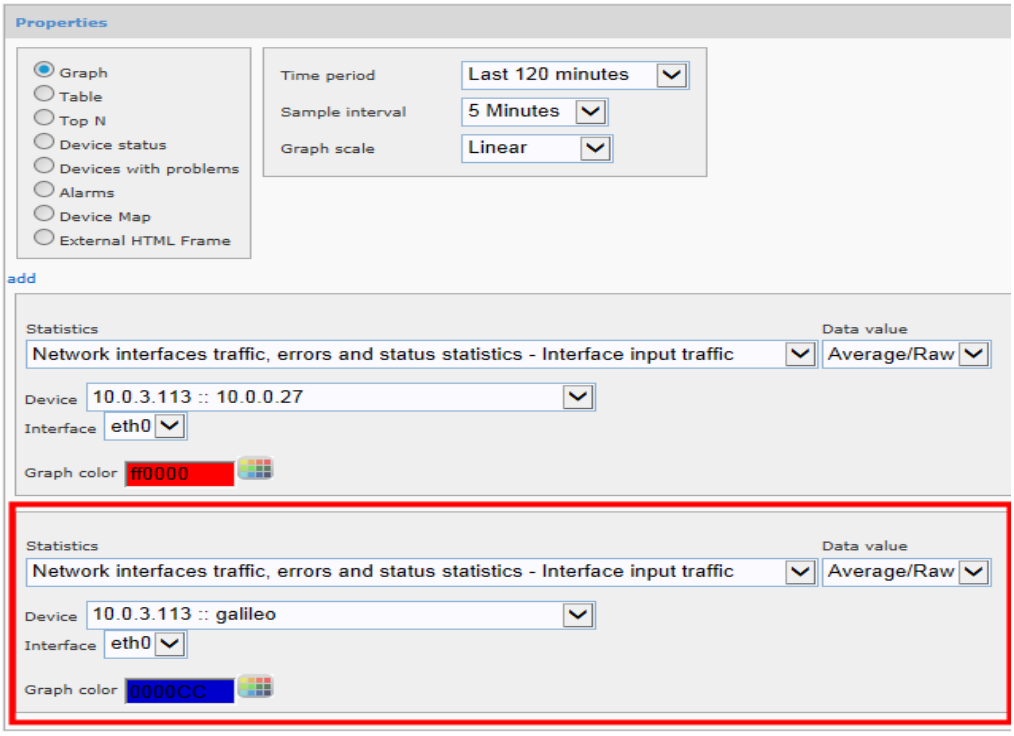


Figure 55: Adding a new variable to the existing graph

5. To add additional variable to the graph, repeat steps 2 and 3 above.
6. When you have finished configuring the settings for the new object, click the ***OK*** button (✔) in the ***Properties*** frame to create and view the report page containing both objects (Figure 56).

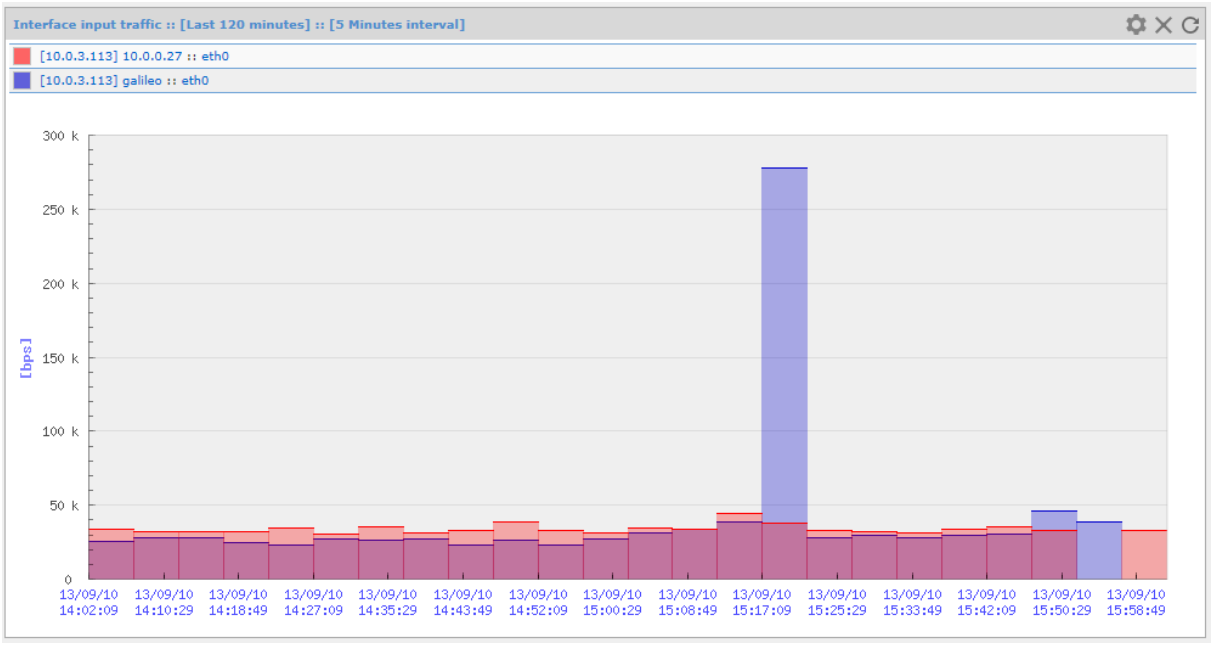


Figure 56: Viewing a graph chart containing two variables

4.3.1 Creating Map Report Page

This section describes how to add and configure a map report page, which is configured under custom report pages.

1. Click the ***Reports*** tab in the main window to display the **Reports** page (Figure 57).

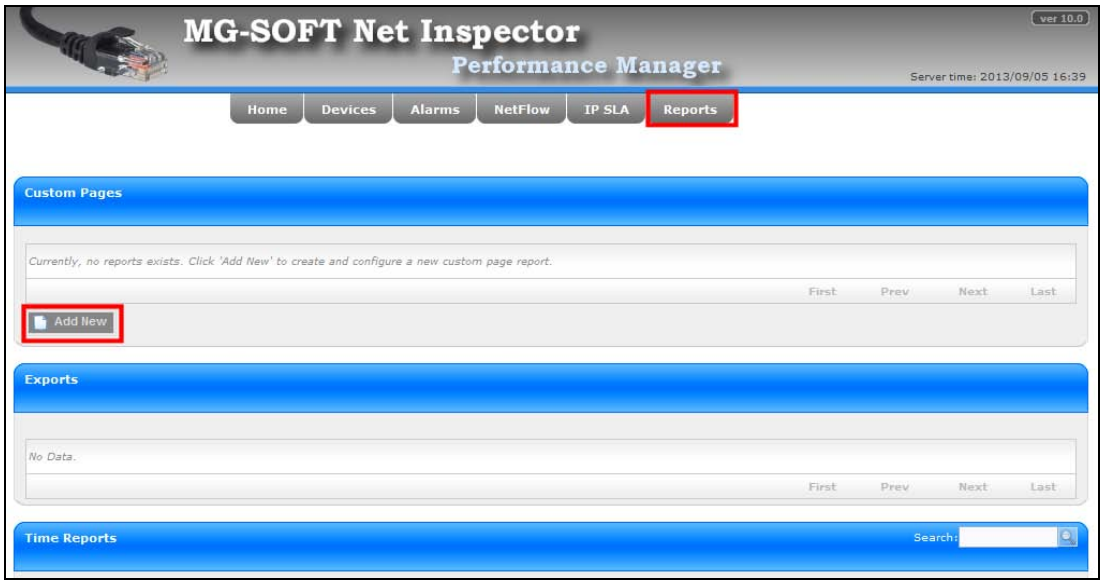


Figure 57: The Reports home page

2. In the ***Custom pages*** frame, click the ***Add New*** button (Figure 57) to start configuring a custom report page.
3. The ***Custom Report Page*** configurator appears (Figure 58).

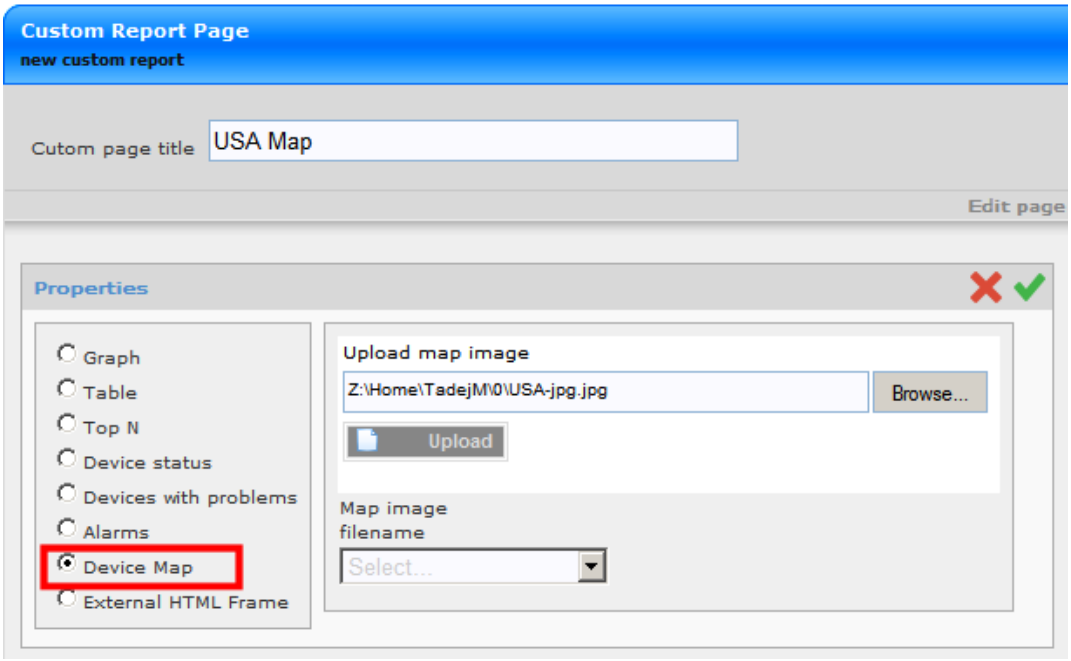


Figure 58: Device map report configurator

4. Into the ***Custom page title*** input line, enter the title of the custom report page you are creating.
5. A custom report page can contain 1, 2 or 3 columns. Select the desired number of columns from the ***Number of columns*** drop-down list in the **Edit Page Layout** drop-down frame (Figure 46).
6. If the map you want to load is in the **Map image filename** drop-down list in the ***Properties*** frame, proceed to step 8. Otherwise, click the ***Browse*** button next to the **Upload map image** input line and select the image file from your disk.
7. After you have selected the image file you want to use as the map background, click the ***Upload*** button. This also adds the selected image to the **Map image filename** drop-down list.
8. Select the map image you want to load from the ***Map image filename*** drop-down list. The selected map image will be displayed below the ***Properties*** frame, with a list of devices displayed on the right hand-side (Figure 59).
9. From the list on the right hand-side, drag the devices you want to monitor and drop them to the desired position on the map (Figure 59).

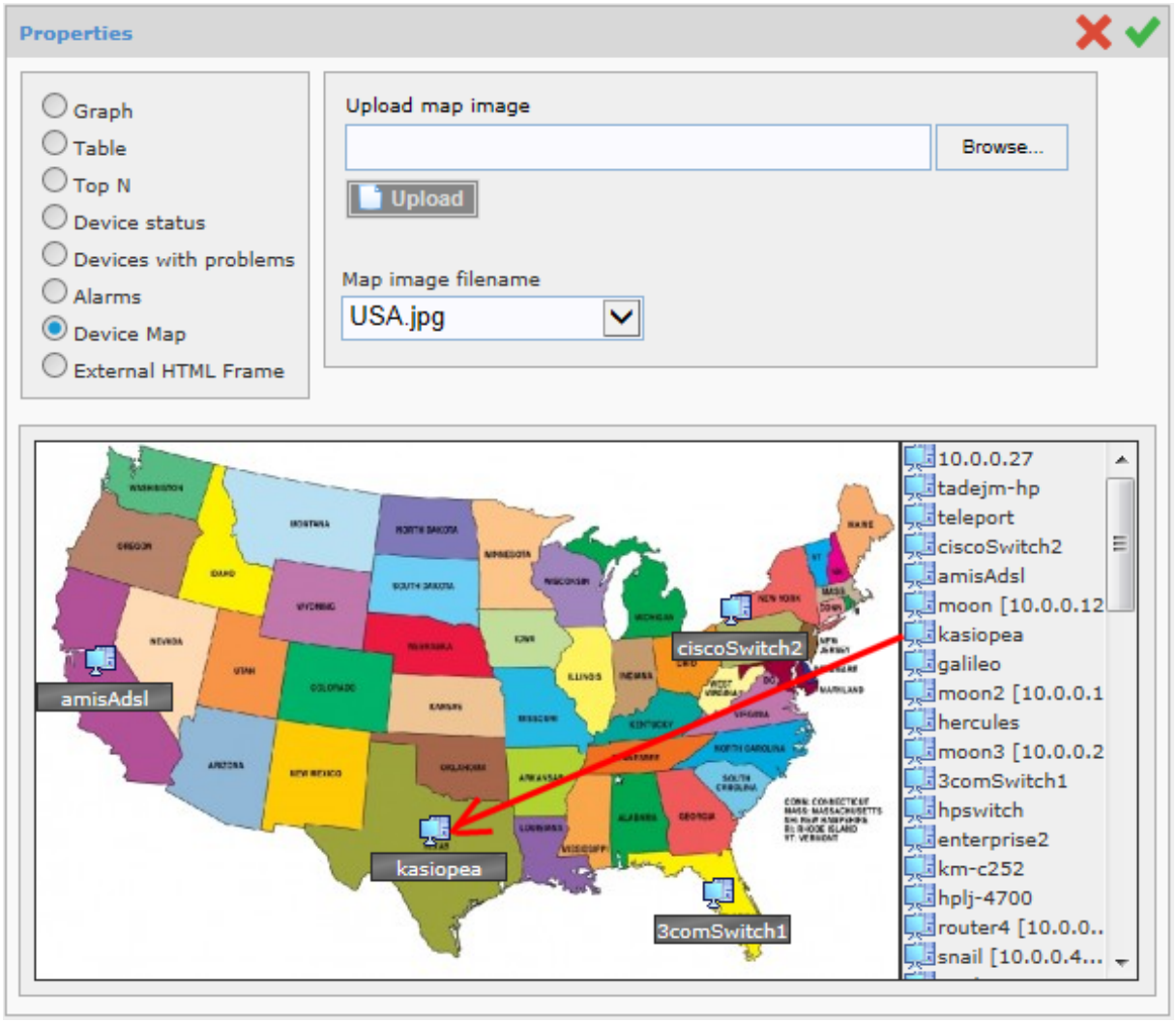


Figure 59: Device map report configurator (second page)

10. When you have finished placing devices on the image, click the ***OK*** button (✔) in the titlebar of the ***Properties*** frame to create and view the newly created report page containing one object (Device map).

Figure 60: Viewing a device map report page.

4.3.2 Monitoring Devices on Map

Device map report pages let you monitor the status of included devices and alarms associated with them.

The color of a device icon background (Figure 60) reflects the current status of the given device, using the following color scheme:

green - device is up
red - device is down
gray - device is not monitored

In addition, a symbol representing the severity level of the most severe alarm that currently exists on the given device (if any) is shown on the device icon background. The alarm severity symbols are described here.

Place your mouse pointer over a device icon to see more details about the corresponding device in a tooltip (device name, IP address, description) and alarms associated with the device (total number of alarms and the most severe alarm displayed in brackets).

4.4 Creating PDF Reports

Performance Manager can generate reports in Adobe PDF format from all custom report pages as well as from some built-in pages (like the pages showing a device's detailed response time statistics etc).

To create a PDF report from a custom report page, proceed as follows:

1. Click the ***Reports*** tab in the main window to display the **Reports** page (Figure 49).
2. In the **Custom report pages** frame, click the name of the custom report page you want to export to PDF format. This displays the custom report page.
3. Click the ***Export to PDF*** button in the titlebar of the custom report page (Figure 61).

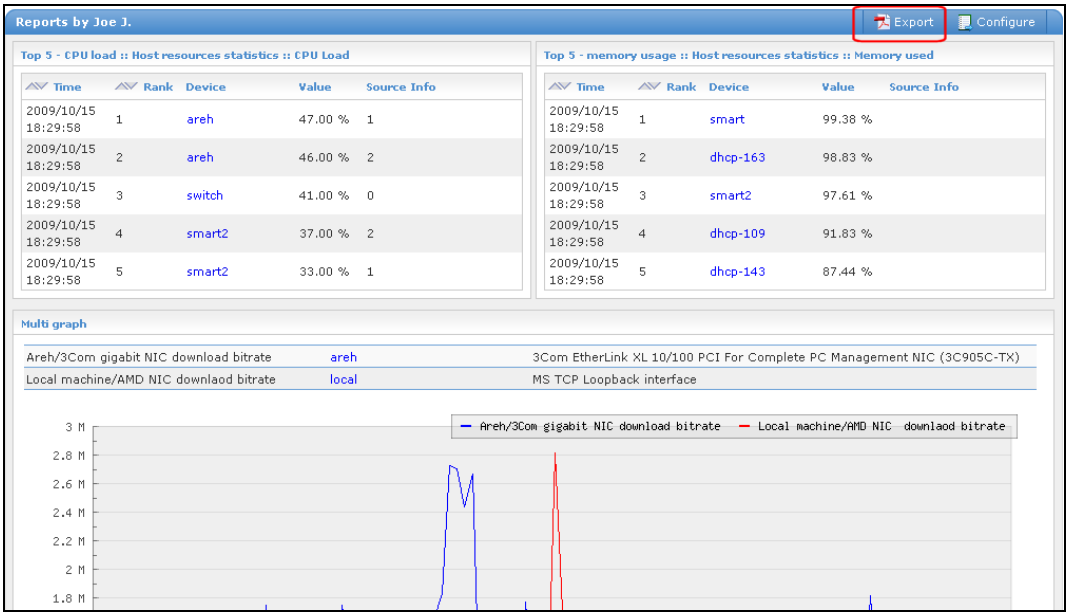

Reports by Joe J.
Export
Configure
Top 5 - CPU load :: Host resources statistics :: CPU Load
Time Rank Device Value Source Info
2009/10/15 18:29:58 1 areh 47.00 % 1
2009/10/15 18:29:58 2 areh 46.00 % 2
2009/10/15 18:29:58 3 switch 41.00 % 0
2009/10/15 18:29:58 4 smart2 37.00 % 2
2009/10/15 18:29:58 5 smart2 33.00 % 1
Top 5 - memory usage :: Host resources statistics :: Memory used
Time Rank Device Value Source Info
2009/10/15 18:29:58 1 smart 99.38 %
2009/10/15 18:29:58 2 dhcp-163 98.83 %
2009/10/15 18:29:58 3 smart2 97.61 %
2009/10/15 18:29:58 4 dhcp-109 91.83 %
2009/10/15 18:29:58 5 dhcp-143 87.44 %
Multi graph
Areh/3Com gigabit NIC download bitrate areh 3Com EtherLink XL 10/100 PCI For Complete PC Management NIC (3C905C-TX)
Local machine/AMD NIC downlaod bitrate local MS TCP Loopback interface
Areh/3Com gigabit NIC download bitrate
Local machine/AMD NIC downlaod bitrate
3 M
2.8 M
2.6 M
2.4 M
2.2 M
2 M
1.8 M

Figure 61: Generating a PDF report

4. A PDF file is generated from the given page and displayed in the new window or new tab in the web browser (Figure 62) provided that PDF viewer is installed. Once the PDF file is created it is listed and accessible in the PDF Reports frame in the Reports page (Figure 63).

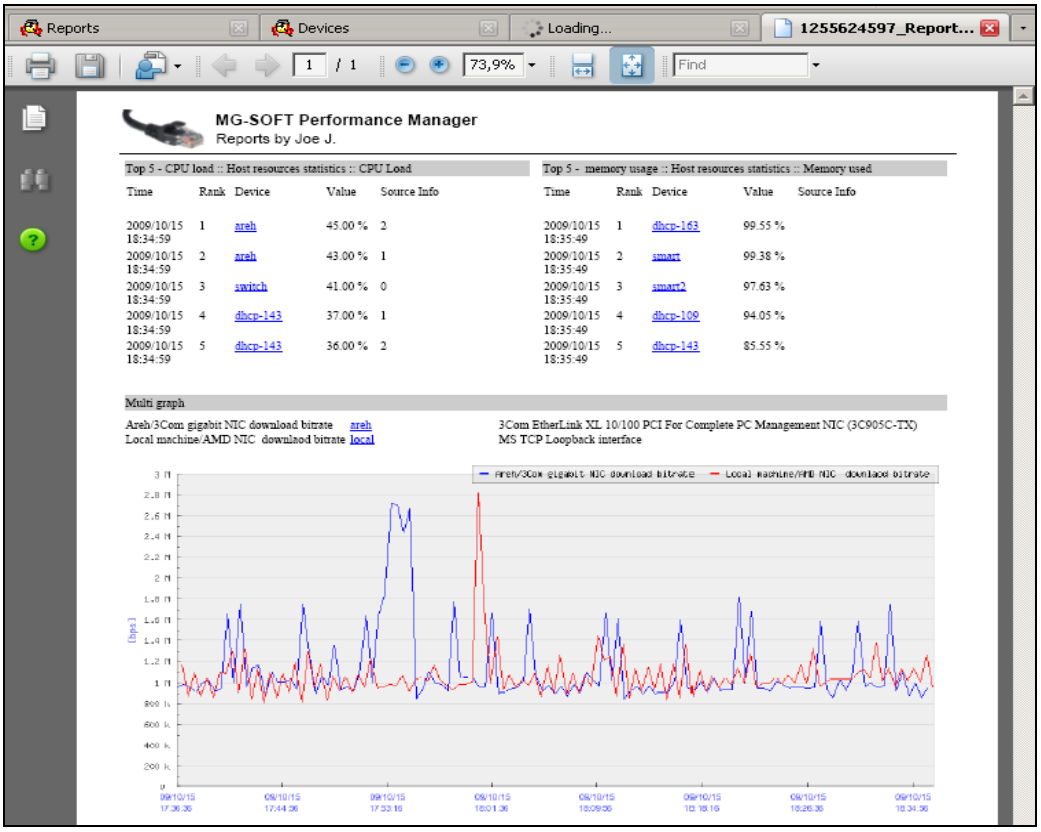

Reports
Devices
Loading...
1255624597_Report...
MG-SOFT Performance Manager
Reports by Joe J.
Top 5 - CPU load :: Host resources statistics :: CPU Load
Top 5 - memory usage :: Host resources statistics :: Memory used
Multi graph
Areh/3Com gigabit NIC download bitrate
Local machine/AMD NIC download bitrate
3Com EtherLink XL 10/100 PCI For Complete PC Management NIC (3C905C-TX)
MS TCP Loopback interface

Figure 62: Viewing Custom report page in PDF format

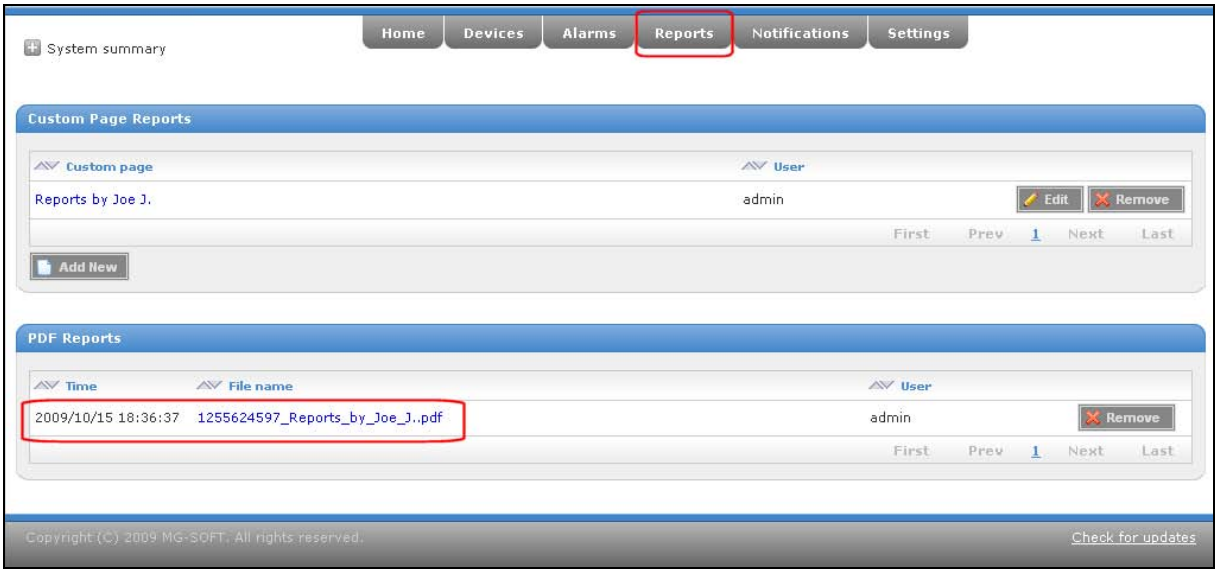


Figure 63: A PDF report in the Reports page

5 VIEWING NUMBER OF MONITORED OBJECTS

MG-SOFT Net Inspector is available in four editions; LITE, WorkGroup, Enterprise and Carrier Edition. For details, please visit the following web page:

http://www.mg-soft.com/netinsp-editions.html

Only Net Inspector WorkGroup, Enterprise and Carrier Editions incorporate performance Manager and NetFlow functionality. Among others, these two editions differ regarding the number of **objects** that can be monitored. An object in this context is either a monitored network **device,** a monitored network **interface** or a monitored **storage volume** (disk partition). You can select which interfaces and storage volumes on devices you want to monitor. When the total number of monitored objects supported by your license is reached, no additional objects can be monitored.

To view the total number of monitored devices by Net Inspector, and the total number of objects monitored by each Performance Manager polling engine, proceed as follows:

In Net Inspector Client, select the ***Help/About*** command from the main menu.